

Entanglement sampling and applications

Frédéric Dupuis,^{1,2,*} Omar Fawzi,^{2,†} and Stephanie Wehner^{3,4,‡}

¹Department of Computer Science, Aarhus University, Åbøgade 34, 8200 Aarhus, Denmark

²Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland

³Centre for Quantum Technologies, National University of Singapore, 2 Science Drive 3, 117543 Singapore

⁴School of Computing, National University of Singapore, 13 Computing Drive, 117417 Singapore

(Dated: May 8, 2013)

A natural measure for the amount of quantum information that a physical system E holds about another system $A = A_1, \dots, A_n$ is given by the min-entropy $H_{\min}(A|E)$. Specifically, the min-entropy measures the amount of entanglement between E and A , and is the relevant measure when analyzing a wide variety of problems ranging from randomness extraction in quantum cryptography, decoupling used in channel coding, to physical processes such as thermalization or the thermodynamic work cost (or gain) of erasing a quantum system. As such, it is a central question to determine the behaviour of the min-entropy after some process \mathcal{M} is applied to the system A . Here we introduce a new generic tool relating the resulting min-entropy to the original one, and apply it to several settings of interest.

- A simple example of such a process is the one of *sampling*, where a subset S of the systems A_1, \dots, A_n is selected at random. The question is then to quantify the entanglement that E has with the selected systems A_S , i.e., $H_{\min}(A_S|ES)$ as a function of the original $H_{\min}(A|E)$. This has two applications by itself. First, it directly provides the first local quantum-to-classical randomness extractors for use in quantum cryptography, as well as decoupling operations acting on only a small fraction A_S of the input A . Moreover, it gives lower bounds on the dimension of k -out-of- n fully quantum random access encodings.
- Another natural example of such a process is a measurement in e.g., BB84 bases commonly used in quantum cryptography. We establish the first entropic uncertainty relations with quantum side information that are nontrivial whenever E is not maximally entangled with A .
- As a consequence, we are able to prove optimality of quantum cryptographic schemes in the noisy-storage model (NSM). This model allows for the secure implementation of two-party cryptographic primitives under the assumption that the adversary cannot store quantum information perfectly. A special case is the bounded-quantum-storage model (BQSM) which assumes that the adversary's quantum memory device is noise-free but limited in size. Ever since the inception of the BQSM [19], it has been a vexing open question to determine whether security is possible as long as the adversary can only store strictly less than the number of qubits n transmitted during the protocol. Here, we show that security is even possible as long as the adversary's device is not larger than $n - O(\log^2 n)$ qubits, which finally settles the fundamental limits of the BQSM.

I. INTRODUCTION

A central task in quantum theory is to effectively quantify the amount of information that some system E holds about some classical or quantum data A . For classical data, i.e., A is a string $X^n = X_1, \dots, X_n$, the *min-entropy* $H_{\min}(X^n|E)$ forms a particularly relevant measure because it determines the length of a secure key that can be obtained from X^n . This is the setting typically considered in quantum key distribution where E is some information that an adversary Eve has gathered during the course of the protocol, and X^n is the so-called raw key. More precisely, the maximum number ℓ of (almost) random bits¹ that can be obtained from X^n that are both uniform and uncorrelated from E obeys $\ell \approx H_{\min}(X^n|E)$, if E is classical [34] and quantum [50]. The process by which such randomness is obtained is known as *randomness extraction* (see [58] for a survey) or *privacy amplification*. Classically, a (strong) randomness extractor is simply a set of functions $\mathcal{F} = \{f : \{0, 1\}^n \rightarrow \{0, 1\}^\ell\}$ such that for almost all functions $f \in \mathcal{F}$, its output $f(X^n)$ is close to uniform and uncorrelated from the adversary, even if he learns which function was applied. That is, the output is of the form $\rho_{f(X)EF} \approx \text{id}/2^n \otimes \rho_{EF}$. A well known example of such a set \mathcal{F} is a set of two-universal hash functions which are used in quantum cryptography to turn a raw key X^n into a secure key $f(X^n)$. The min-entropy also has a very intuitive interpretation as it can be expressed as

*dupuis@cs.au.dk

†ofawzi@phys.ethz.ch

‡steph@locc.la

¹ We restrict ourselves to bits in the introduction, however, all our results also apply to higher dimensional alphabets.

$H_{\min}(X^n|E) = -\log P_{\text{guess}}(X^n|E)$ where $P_{\text{guess}}(X^n|E)$ is the probability that the adversary manages to guess X^n maximized over all measurements on E [36].

What can we say in the case of quantum data A ? It turns out that the fully quantum min-entropy $H_{\min}(A|E)$ provides us with a similarly useful way to quantify the amount of information that E holds about A . Its first significance is to quantum cryptography where E is again held by an adversary. More specifically, it has been shown that a quantum-to-classical extractor (QC-extractor) can produce exactly $\ell \approx H_{\min}(A|E) + \log |A|$ classical bits which are uniform and uncorrelated from E [11]. Instead of applying functions to a classical string, a QC-extractor consists of a set of projective measurements on A giving a classical string as a measurement outcome. Such extractors form a useful tool in two-party quantum cryptography where one might have an estimate of $H_{\min}(A|E)$, but not of the min-entropy of any classical string X^n produced from A . Thus $H_{\min}(A|E)$ is directly related to the amount of cryptographic randomness that can be produced from A .

More generally, the min-entropy is of significance in quantum information theory where it quantifies the number of qubits of A that can be decoupled from E [25, 30]. A decoupling operation is given by a quantum operation $\mathcal{K}_{A \rightarrow B}$ on the system A that (approximately) transforms a state ρ_{AE} to $\tau_B \otimes \rho_E$, where τ_B depends only on \mathcal{K} but not on ρ_A . When $\tau_B = \text{id}/|B|$ is the maximally mixed state, the operation $\mathcal{K}_{A \rightarrow B}$ again generates randomness with respect to E and can hence be understood as a fully quantum-to-quantum extractor (QQ-extractor). When decoupling is used in quantum information theory, E is typically the environment of a channel $\mathcal{N}_{\bar{A} \rightarrow B}$ acting on half of a maximally entangled state $\Phi_{A\bar{A}}$, and the number of qubits that can be decoupled relates directly to the number of qubits that can be transmitted correctly through the channel $\mathcal{N}_{\bar{A} \rightarrow B}$ (see [24] for an in-depth exposition). Recently, the min-entropy has also gained prominence in related areas such as the study of thermalization [23, 33] and well as the thermodynamics work cost (or gain!) of erasing a quantum system [22].

It turns out that the fully quantum min-entropy also enjoys a very appealing operational interpretation [36]. More precisely,

$$H_{\min}(A|E) = -\log |A| \max_{\Lambda_{E \rightarrow \bar{A}}} F(\Phi_{A\bar{A}}^N, \text{id}_A \otimes \Lambda_{E \rightarrow \bar{A}}(\rho_{AE}))^2, \quad (1)$$

where F is the fidelity (see below) and $\Phi_{A\bar{A}}^N$ is the normalized maximally entangled state across A and \bar{A} . That is, $H_{\min}(A|E)$ measures how close ρ_{AE} can be brought to the maximally entangled state by performing a quantum operation on E . Intuitively, this quantifies how close the adversary E can bring himself to being quantumly maximally correlated with A — exactly analogous to maximizing his classical correlations by trying to guess X^n .

A. Results

Given the significance of the min-entropy in quantum information, it is a natural question to ask how the min-entropy changes if we apply a quantum operation \mathcal{M} to A . More precisely, one might ask how $H_{\min}(\mathcal{M}(A)|E)$ relates to $H_{\min}(A|E)$, for some completely positive trace preserving map \mathcal{M} . At present, we know that the min-entropy satisfies $H_{\min}(\mathcal{M}(A)|E) \geq H_{\min}(A|E)$ if \mathcal{M} is unital [54]. Can we make more refined statements?

Of particular interest to us is the case where the quantum system consist of n qudits $A^n = A_1, \dots, A_n$. Our main result is to establish the following very general theorem for maps \mathcal{M} with the property that we can diagonalize $((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) = \sum_{s \in \{0, \dots, d^2-1\}} \lambda_s \Phi_s$ where $A^n = A_1, \dots, A_n$, $d = |A_j|$ is the dimension of one of the individual qudits, $\Phi_{A^n \bar{A}^n}$ is again the maximally entangled state, and $\{\Phi_s\}_s$ is a basis for the space $A^n \otimes \bar{A}^n$ consisting of maximally entangled vectors (see Sections II and Section III for precise definitions and statement of the theorem). In terms of the smooth min-entropy H_{\min}^ε , which, loosely speaking, is equal to the min-entropy except with error probability ε , our first contribution can be stated as

- **Main result (Informal)** For any partition of $\{0, \dots, d^2-1\}^n = \mathfrak{S}_+ \cup \mathfrak{S}_-$ into subsets $\mathfrak{S}_+, \mathfrak{S}_-$ we have $2^{-H_{\min}^\varepsilon(\mathcal{M}(A^n)|E)} \lesssim \sum_{s \in \mathfrak{S}_+} \lambda_s 2^{-H_{\min}(A^n|E)} + (\max_{s \in \mathfrak{S}_-} \lambda_s) d^n$.

At first glance, our condition on the maps \mathcal{M} may seem rather unintuitive and indeed restrictive. Yet, it turns out that many interesting maps do indeed satisfy these conditions, allowing us to establish the following results.

Entanglement sampling In the study of classical extractors, a goal was to construct families of functions f that are *locally computable* [59]. That is, if our goal were to extract only a very small number of key bits from a long string X^n of length n , one might wonder whether this can be done efficiently in the sense that the functions f depend only on a small number of bits of X^n . Classically, a very beautiful method to answer this question is to show that the min-entropy can in fact be *sampled* [47, 59]. That is, if we choose a subset S of the bits at random, then the min-entropy of

the bits X_S in that subset S obeys

$$H_{\min}(X_S|ES) \gtrsim |S|R(H_{\min}(X^n|E)/n), \quad (2)$$

for some function R . The function R can be understood as a rate function that determines the relation of the original min-entropy rate $\frac{H_{\min}(X^n|E)}{n}$ to the min-entropy rate on a subset S of the bits. In other words, min-entropy sampling says that if X^n is hard to guess, then even given the choice of subset S it is tricky for the adversary to guess X_S . To see why this yields the desired functions f note that one way to construct a randomness extractor would be to first pick a random subset S , and then apply an arbitrary extractor to the much shorter bit string X_S . In the classical literature, this is known as the sample-then-extract approach [59].

Inspired by the classical results of Vadhan [59], it is a natural question whether there exists QC-extractors which are efficient in the sense that the measurements $M \in \mathcal{M}$ only act on a small number of qubits of $A^n = A_1, \dots, A_n$. Or, even more generally, whether there exist decoupling operations which depend on only very few qubits. As before, one way to answer this question in generality is to show that even the fully quantum min-entropy can be sampled - that is, that *entanglement* can be sampled.

- **Entanglement sampling (Informal)** Entanglement sampling is possible for any quantum state $\rho_{A^n E}$, i.e., $H_{\min}^\varepsilon(A_S|ES) \gtrsim |S|R(H_{\min}(A^n|E)/n)$ for the rate function R plotted in Figure 1. See Theorem 2 for a precise statement.

It should be noted that even the case of standard min-entropy sampling of a classical string X^n , but quantum side information E has proved challenging. The results of [6] imply that sampling of classical strings is possible when the distribution over the strings X^n is uniform (i.e., $\rho_{X^n E} = (1/2^n) \sum_{x \in \{0,1\}^n} |x\rangle\langle x| \otimes \rho_E^x$), and the size of E is bounded, and [38] has shown that sampling of blocks (but not individual bits) is possible. This was later refined in [63] to show that bitwise sampling is also possible (see Figure 1 for a comparison of the rate function). Very roughly, the techniques used in [63] relate the adversary's ability to guess the string X^n to his ability to guess the XOR of bits in the string. Clearly, in the case of fully quantum A^n such techniques cannot be used as it is indeed unclear what the XOR of qubits even means.

As this is the first result on entanglement sampling, it required entirely novel techniques. More precisely, it inspired the even more general theorem sketched above, from which entanglement sampling follows by choosing an appropriate map \mathcal{M} . As a byproduct, using the same techniques, we also obtain a stronger statement of sampling a classical string X^n with respect to a quantum system E in the sense that the rate R is improved (see Figure 1 for a comparison). What's more, we are able to show an even more precise statement in terms of the entropy $H_2(A^n|E)_\rho$ - without any ε error terms. Classically, this quantity is known as the (conditional) collision entropy. In general, it is very closely related to the min-entropy, and in fact enjoys a very similar operational interpretation. More specifically, it can be expressed in the same form as (1) where the optimization over all quantum operations $\Lambda_{E \rightarrow \bar{A}^n}$ is replaced by the so-called *pretty good recovery* map $\Lambda_{E \rightarrow \bar{A}^n}^{\text{pg}}$ which is close to optimal [4].

Application to quantum random access codes Another application of our entanglement sampling result is to the fully quantum random access codes. Previous works have considered encodings of n classical bits $X^n = X_1, \dots, X_n$ into quantum states $\rho_E^{X^n}$ such that any desired bit can be retrieved with a particular success probability p [2, 45]. This was later generalized to retrieving any subset of k bits from the encoding [6]. The goal of [6, 45] was to derive a bound on the necessary dimension of $\rho_E^{X^n}$ as a function of p when the string X^n was chosen uniformly at random. Here, we prove dimension bounds for encoding n qubits $A^n = A_1, \dots, A_n$ when we desire to recover any subset of k qubits with a particular fidelity. Or, read in the opposite direction, we establish a bound on the fidelity as a function of the dimension (see Section IV C).

Uncertainty relations Another consequence of our main result is a new uncertainty relation with quantum side information [9] for measurements of n qubits $A^n = A_1, \dots, A_n$ in randomly chosen BB84 [7] bases. Apart from the foundational consequences, such relations have found use in verifying the presence of entanglement [49] as well as in quantum cryptography (see e.g., [11]). Our result establishes the first entropic uncertainty relation with quantum side-information that uses a high-order entropy like the min-entropy and that is nontrivial as soon as the system being measured is not maximally entangled with the observer E . In other words, this shows a quantitative bound on the probability of successfully guessing the measurement outcome that is nontrivial as soon as $H_{\min}(A^n|E) > -n$.²

² The fully quantum min-entropy can be negative up to $H_{\min}(A^n|E) = -n$ if $\rho_{A^n E}$ is the maximally entangled state.

- **High-order entropic uncertainty relation for BB84 bases** If X^n is obtained by measuring the system A^n in a random BB84 bases Θ^n , we have $H_{\min}(X^n|E\Theta^n) \geq n \cdot \frac{1}{2}\gamma\left(\frac{H_{\min}(A^n|E)}{n}\right)$, where the function γ is plotted in Figure 2. See Theorem 10 and Corollary 11 for precise statements.

We also prove uncertainty relations for qudit-wise measurements in mutually unbiased bases in Theorem 12. Again, these results follow from our very general theorem sketched above, this time for a map \mathcal{M} that represents randomly chosen measurements.

Applications to the noisy-storage model Our new uncertainty relations have several interesting applications to cryptography. The goal of two-party cryptography is to enable Alice and Bob to solve tasks in cooperation even if they do not trust each other. A classic example of such tasks are bit commitment and oblivious transfer. Unfortunately, it has been shown that even using quantum communication, none of these tasks can be implemented securely without making assumptions [15, 17, 21, 40, 41, 44]. What makes such tasks more difficult than quantum key distribution is that Alice and Bob cannot collaborate to check on any eavesdropper. Instead, each party has to fend for itself.

Nevertheless, because two-party computation is such a central part of modern cryptography, one is willing to make *assumptions* on how powerful an attacker can be in order to implement them securely. Classically, such assumptions generally take the form of computational assumptions, where we assume that a particular mathematical problem cannot be solved in polynomial time. Here, we consider *physical* assumptions that can enable us to solve such tasks. In particular, can the sole assumption of a limited storage device lead to security [43]? This is indeed the case and it was shown that security can be obtained if the attacker's *classical* storage is limited [16, 43]. Yet, apart from the fact that classical storage is cheap and plentiful, assuming a limited classical storage has one rather crucial caveat: If the honest players need to store n classical bits to execute the protocol in the first place, *any* classical protocol can be broken if the attacker can store more than roughly n^2 bits [26]. Motivated by this unsatisfactory gap, it was thus suggested to assume that the attacker's *quantum* storage was bounded [7, 12, 18–20], or, more generally, noisy [37, 51, 60]. The central assumption of the noisy-storage model is that during waiting times Δt introduced in the protocol, the attacker can keep quantum information only in his noisy quantum storage device; otherwise he is all-powerful (see Section IV E).

The assumption of bounded or noisy quantum storage offers significant advantages in that the proposed protocols do not require any quantum storage at all to be implemented by the honest parties. They are typically based on BB84 [37] or six-state [11] encodings, and indeed the first implementation of a bit commitment protocol has recently been performed experimentally [46]. So far it was known that there exist protocols that send n qubits encoded in either the BB84 or six-state encoding, and that are secure as long as the adversary can only store strictly less than $n/2$ or $2n/3$ noise-free qubits respectively.

Using our new techniques, we are able to show security of the primitive called *weak string erasure* [37] (see Section IV E), which in turn can be supplemented with additional classical or quantum communication [64] to obtain primitives such as bit commitment.

- **Application 1: Bounded storage** There exists a weak string erasure protocol transmitting n qubits that is secure as long as the adversary can store at most strictly less than $n - O(\log^2 n)$ qubits. The protocol does not require any quantum memory to be executed, and merely requires simple quantum operations and measurements. See Theorem 15 for a precise statement.

It should be noted that no such protocol can be secure as soon as the adversary can store n qubits, so our result is essentially optimal. Our result highlights the sharp contrast between the classical and the quantum bounded storage model and answers the main open question in the BQSM. The noisy-storage model offers an advantage over the case of bounded-storage not only for implementations using high-dimensional encodings such as the infinite-dimensional states sent in continuous variable experiments, but allows security even for arbitrarily large storage devices as long as the noise is large enough.³ Essentially, the noisy-storage model captures our intuition that security should be linked to how much information the adversary can store in his quantum memory. The first proofs linked

³ For information theory experts, we note that security in the noisy-storage model does not directly follow from security in the bounded-storage model because the entanglement cost of a channel [8] is not equal to its quantum capacity. The entanglement cost measures the number of noise free channels (bounded storage) needed to simulate a certain number of noisy channels, in the presence of classical communication. As such, it allows properties of noisy channels to be derived from properties of noiseless channels: a certain amount of noisy channels cannot be used to accomplish a certain task (like sending a certain number of qubits with a given fidelity) because otherwise also some number of noise free channels could be used by simulating the noisy ones.

security to the classical capacity [37], the entanglement cost [8] and finally the quantum capacity [11]. The latter result used a protocol based on six-state encodings.

- **Application 2: Noisy storage** We significantly push the boundaries regarding when security is possible in the noisy-storage model (see Section IV E). Furthermore, we link security of a BB84-based protocol to the quantum capacity of the adversary's storage device for the first time. See Theorem 14 for a precise statement.

II. PRELIMINARIES

A. Basic concepts and notation

In quantum mechanics, a system such as Alice's or Bob's labs are described mathematically by *Hilbert spaces*, denoted by A, B, C, \dots . Here, we follow the usual convention in quantum cryptography and assume that all Hilbert spaces are finite-dimensional. We write $|A|$ for the dimension of A . A system of n qudits is also denoted as $A^n = A_1, \dots, A_n$, where we also use $|A|$ to denote the dimension of one single qudit in A^n . The set of linear operators on A is denoted by $\mathcal{L}(A)$, and we write $\text{Herm}(A)$ and $\text{Pos}(A)$ for the set of hermitian and positive semidefinite operators on A respectively. We denote the adjoint of an operator M by M^\dagger . A *quantum state* ρ_A is an operator $\rho_A \in \mathcal{S}(A)$, where $\mathcal{S}(A) = \{\sigma_A \in \text{Pos}(A) \mid \text{Tr}(\sigma_A) = 1\}$. We will often make use of *operator inequalities*: whenever $X, Y \in \text{Herm}(A)$, we write $X \leq Y$ to mean that $Y - X \in \text{Pos}(A)$. A quantum operation is given by a completely positive map $\mathcal{M} : \mathcal{L}(A) \rightarrow \mathcal{L}(C)$. A map \mathcal{M} is said to be completely positive if for any system B and $X \in \text{Pos}(A \otimes B)$ we have $(\mathcal{M} \otimes \text{id})(X) \geq 0$ (see [29] for properties of quantum channels).

Throughout, we use the shorthand $[d] = \{0, 1, \dots, d-1\}$. We will follow the convention to use H to denote the unitary that takes the computational $\{|0\rangle, |1\rangle\}$ to the Hadamard basis: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. When considering n qubits, we also use $H^{\theta^n} = H^{\theta_1} \otimes \dots \otimes H^{\theta_n}$ for the unitary defining the basis $\theta^n \in \{0, 1\}^n$.

B. Entropies

Next to its operational interpretation given in (1), the *conditional min-entropy* of a state $\rho_{AB} \in \mathcal{S}(AB)$ can also be expressed as

$$H_{\min}(A|B)_\rho = \max_{\sigma_B \in \mathcal{S}(B)} H_{\min}(A|B)_{\rho|\sigma} \text{ with } H_{\min}(A|B)_{\rho|\sigma} = \max \{ \lambda \in \mathbb{R} : 2^{-\lambda} \cdot \text{id}_A \otimes \sigma_B \geq \rho_{AB} \}, \quad (3)$$

where the symbol id_A refers to the identity on A . We use the subscript ρ to emphasize the state ρ_{AB} of which we evaluate the min-entropy. The smoothed version is defined by $H_{\min}^\epsilon(A|B)_\rho = \max_{\tilde{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}$, where $\mathcal{B}^\epsilon(\rho)$ is the set of states at a distance at most ϵ from ρ . We use the purified distance as the distance measure [55]. We refer to [54] for a review of the properties of the min-entropy.

It is simpler to state our results in terms of the related collision entropy defined for any $\rho_{AB} \in \text{Pos}(A \otimes B)$ by

$$H_2(A|B)_\rho = -\log \text{Tr} \left[\left(\rho_B^{-1/4} \rho_{AB} \rho_B^{-1/4} \right)^2 \right]. \quad (4)$$

The two entropy measures H_{\min} and H_2 are closely related as shown in Lemmas 17, 18 and 19. The collision entropy also has an appealing operational interpretation [10] as

$$H_2(A|B)_\rho = -\log \left(|A| F(\Phi_{AA'}^N, \text{id}_A \otimes \Lambda_{E \rightarrow A'}^{\text{pg}}(\rho_{AE}))^2 \right), \quad (5)$$

where $F(\sigma_1, \sigma_2) = \text{Tr}(\sqrt{\sqrt{\sigma_1} \sigma_2 \sqrt{\sigma_1}})$ is the fidelity, and $\Lambda_{E \rightarrow A'}^{\text{pg}}$ is the *pretty good recovery* map [4] (see Section C of the appendix). Finally, we use the binary entropy function $h(x) = -x \log x - (1-x) \log(1-x)$.

For the curious reader, we note that the quantity (5) has indeed also appeared in a slightly different guise in the context of norms employed for the study of mixing properties of quantum channels [53]. Specifically, we have $\|\rho_{AB}\|_{\sigma,2} = 2^{-H_2(A|B)_\rho}$ with $\sigma = \text{id}_A \otimes \rho_B^{-1}$ for the norm $\|\cdot\|_{\sigma,2}$ defined in [53].

C. A convenient basis

Throughout, we make use of a very convenient basis of maximally entangled states for the space $A \otimes \bar{A}$ where $\bar{A} \simeq A$. The (unnormalized) maximally entangled state

$$|\Phi\rangle_{A\bar{A}} = \sum_a |a\rangle_A \otimes |a\rangle_{\bar{A}} \quad (6)$$

will play an important role in our analysis. Here, the vectors $|a\rangle$ label the standard basis of A . We use $|\Phi^N\rangle_{A\bar{A}}$ to denote the normalized version $|\Phi^N\rangle_{A\bar{A}} = \frac{1}{\sqrt{|A|}} |\Phi\rangle_{A\bar{A}}$. We repeatedly use the following properties. For any operators X and Y acting on A , we have

$$\text{Tr}[XY] = \text{Tr}[X \otimes \mathbb{T}(Y) \Phi_{A\bar{A}}] \quad (7)$$

where \mathbb{T} denotes the transpose map in the standard basis and $\Phi_{A\bar{A}} = |\Phi\rangle\langle\Phi|_{A\bar{A}}$. Moreover, we have

$$(X \otimes \text{id}_{\bar{A}})|\Phi\rangle_{A\bar{A}} = (\text{id}_A \otimes \mathbb{T}(X))|\Phi\rangle_{A\bar{A}}. \quad (8)$$

Using (7) and (8) one can naturally construct an orthogonal basis of $A\bar{A}$ by applying unitary transformations to $|\Phi\rangle$ that are orthogonal with respect to the Hilbert-Schmidt inner product. Define for $s \in [|A|^2]$, $|\Phi_s\rangle = (W_s \otimes \text{id})|\Phi\rangle_{A\bar{A}}$ where W_s denote the generalized Pauli operators (see e.g., [3]), sometimes also called Weyl operators. In fact, all our results would hold for any unitary operators W_s that are orthogonal with respect to the Hilbert-Schmidt inner product. We again use $\Phi_s = |\Phi_s\rangle\langle\Phi_s|$.

In particular for $|A| = 2$, W_0, W_1, W_2, W_3 are the Pauli operators, and we obtain the well-known Bell basis

$$\Phi_0 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad \Phi_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (9)$$

$$\Phi_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \Phi_3 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}. \quad (10)$$

Note that in this numbering scheme, Φ_2 is the singlet.

For $n > 0$, we will denote by A^n the system $\bigotimes_{i=1}^n A_i$, where each A_i is a copy of A . Furthermore, if $S \subseteq \{1, \dots, n\}$, we write A_S to denote $\bigotimes_{i \in S} A_i$. In other words, A^n consists of n copies of the system A , and A_S contains the copies that correspond to indices in S . In such a setting the dimension of the system A is denoted d . We can naturally define for $s \in [d^2]^n$, $|\Phi_s\rangle = \bigotimes_{i=1}^n |\Phi_{s_i}\rangle_{A_i \bar{A}_i}$. We then have that $\{\frac{1}{\sqrt{d^n}} |\Phi_s\rangle\}_s$ is an orthonormal basis of $A^n \bar{A}^n$. For such strings s , we denote $\text{supp}(s) = \{i \in \{1, \dots, n\} : s_i \neq 0\}$ and $|s| = |\text{supp}(s)|$.

III. EVOLUTION OF H_2 UNDER GENERAL MAPS

In this section, we derive constraints on the evolution of the conditional collision entropy H_2 when the system A^n undergoes some transformation described by a completely positive map \mathcal{M} . Our results on entanglement sampling and uncertainty relations are obtained by evaluating this bound for particular channels \mathcal{M} . A statement for the smooth min-entropy follows directly by applying Lemma 19.

Theorem 1. *Let $\mathcal{M}_{A^n \rightarrow C}$ be a completely positive map such that $((\mathcal{M}^\dagger \circ \mathcal{M})_{A^n} \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) = \sum_{s \in [d^2]^n} \lambda_s \Phi_s$ and let $\rho_{A^n E} \in \mathcal{S}(A^n E)$ be a state, where $A^n = A_1, \dots, A_n$ is comprised of n qudits of dimension d . Then for any partition $[d^2]^n = \mathfrak{S}_+ \cup \mathfrak{S}_-$ into subsets \mathfrak{S}_+ and \mathfrak{S}_- , we have*

$$2^{-H_2(C|E)_{\mathcal{M}(\rho)}} \leq \sum_{s \in \mathfrak{S}_+} \lambda_s 2^{-H_2(A^n|E)_\rho} + \left(\max_{s \in \mathfrak{S}_-} \lambda_s \right) d^n. \quad (11)$$

The maps \mathcal{M} of interest typically have some symmetry. For example, if the map \mathcal{M} is invariant under permutations of the n systems A_1, \dots, A_n , then the coefficients λ_s only depend on the type of s , i.e., the number of times each symbol in $[d^2]$ occurs in s . In fact, all of the examples we consider here are such that λ_s only depends on the weight $|s| = |\{i \in [n] : s_i \neq 0\}|$.

Proof. Let $\tilde{\rho}_{A^n E} = \rho_E^{-1/4} \rho_{A^n E} \rho_E^{-1/4}$, and let $\hat{\rho}_{A^n \bar{A}^n} = \text{Tr}_{E\bar{E}}[(\tilde{\rho}_{A^n E} \otimes \top(\tilde{\rho}_{\bar{A}^n \bar{E}}))\Phi_{E\bar{E}}]$. Note that $\hat{\rho}_{A^n \bar{A}^n} \geq 0$ and $\text{Tr}[\hat{\rho}_{A^n \bar{A}^n}] = \text{Tr}[\tilde{\rho}_E^2] = 1$. Furthermore, let \mathcal{M} be such that $\mathcal{M}(\top(X)) = \top(\mathcal{M}(X))$ for all X . Our first goal is to rewrite $H_2(C|E)_\sigma$ in terms of the basis $\{\Phi_s\}_s$. We obtain from (7)

$$\begin{aligned} 2^{-H_2(C|E)_\sigma} &= \text{Tr}[\mathcal{M}(\tilde{\rho}_{A^n E})^2] \\ &= \text{Tr}[(\mathcal{M}(\tilde{\rho}_{A^n E}) \otimes \top(\mathcal{M}(\tilde{\rho}_{\bar{A}^n \bar{E}})))\Phi_{C\bar{C}} \otimes \Phi_{E\bar{E}}] \\ &= \text{Tr}[(\mathcal{M}(\tilde{\rho}_{A^n E}) \otimes \bar{\mathcal{M}}(\top(\tilde{\rho}_{\bar{A}^n \bar{E}})))\Phi_{C\bar{C}} \otimes \Phi_{E\bar{E}}] \\ &= \text{Tr}[(\tilde{\rho}_{A^n E} \otimes \top(\tilde{\rho}_{\bar{A}^n \bar{E}}))((\mathcal{M}^\dagger) \otimes (\bar{\mathcal{M}}^\dagger))(\Phi_{C\bar{C}}) \otimes \Phi_{E\bar{E}}]. \end{aligned}$$

Now by performing a Kraus decomposition of $\bar{\mathcal{M}}^\dagger$ and using (8), we see that $(\text{id}_C \otimes \bar{\mathcal{M}}^\dagger)(\Phi_{C\bar{C}}) = (\mathcal{M}_{A^n \rightarrow C} \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n})$. Thus, we obtain using the condition on \mathcal{M}

$$\begin{aligned} 2^{-H_2(C|E)_\sigma} &= \text{Tr}[(\tilde{\rho}_{A^n E} \otimes \top(\tilde{\rho}_{\bar{A}^n \bar{E}}))((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) \otimes \Phi_{E\bar{E}}] \\ &= \text{Tr}[\hat{\rho}_{A^n \bar{A}^n}((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n})] \\ &= \sum_{s \in [d^2]^n} \lambda_s \text{Tr}[\hat{\rho}_{A^n \bar{A}^n} \Phi_s]. \end{aligned} \tag{12}$$

We now prove the two key constraints on the terms $\text{Tr}[\hat{\rho}_{A^n \bar{A}^n} \Phi_s]$ we will be using. First, we have a global constraint. Note that the set of vectors $\{\frac{1}{\sqrt{d^n}}|\Phi_s\rangle\}_{s \in [d^2]^n}$ forms an *orthonormal* basis and thus $\text{id}_{A^n \bar{A}^n} = \frac{1}{d^n} \sum_{s \in [d^2]^n} \Phi_s$. This yields

$$\sum_{s \in [d^2]^n} \text{Tr}[\hat{\rho}_{A^n \bar{A}^n} \Phi_s] = d^n \text{Tr}[\hat{\rho}_{A^n \bar{A}^n}] = d^n. \tag{13}$$

The second observation concerns the individual terms $\text{Tr}[\hat{\rho}_{A^n \bar{A}^n} \Phi_s]$. For any s ,

$$\begin{aligned} \text{Tr}[\hat{\rho}_{A^n \bar{A}^n} \Phi_s] &= \text{Tr}[\hat{\rho}_{A^n \bar{A}^n} (W_s \otimes \text{id}_{\bar{A}^n}) \Phi_{A^n \bar{A}^n} (W_s^\dagger \otimes \text{id}_{\bar{A}^n})] \\ &= \text{Tr}[(W_s^\dagger \tilde{\rho}_{A^n E} W_s \otimes \top(\tilde{\rho}_{\bar{A}^n \bar{E}})) \Phi_{A^n \bar{A}^n} \otimes \Phi_{E\bar{E}}] \\ &= \text{Tr}[W_s^\dagger \tilde{\rho}_{A^n E} W_s \tilde{\rho}_{A^n E}] \\ &\leq \text{Tr}[\tilde{\rho}_{A^n E}^2] = 2^{-H_2(A^n|E)_\rho}, \end{aligned}$$

using the Cauchy-Schwarz inequality. Also, observe that the positivity of $\hat{\rho}_{A^n \bar{A}^n}$ and Φ_s implies that $\text{Tr}[\hat{\rho}_{A^n \bar{A}^n} \Phi_s] \geq 0$. Thus, we have

$$0 \leq \text{Tr}[\hat{\rho}_{A^n \bar{A}^n} \Phi_s] \leq 2^{-H_2(A^n|E)_\rho}. \tag{14}$$

Applying inequalities (13) and (14) to (12), we obtain the desired result. \square

We remark that equations (13) and (14) are the only properties of the operator $\rho_{A^n E}$ that we are using. This means that the result would also hold for possible operators $\rho_{A^n E}$ that do not correspond to states but still satisfy these conditions.

IV. APPLICATIONS

We now derive several interesting consequences of Theorem 1. All of these follow by making an appropriate choice for the map \mathcal{M} .

A. Quantum-quantum min-entropy sampling

1. Statement

We now state our results on entanglement sampling. The theorem below deals with the following scenario: we have n qudits and we choose a subset of them of size k uniformly at random. We have a lower bound on the collision entropy of the whole state conditioned on some quantum side-information E ; the theorem then gives a lower bound on the conditional collision entropy of the sample. The rate function obtained is plotted in Figure 1 together with an upper bound on the optimal rate function given by a particular example presented in Theorem 5. The same figure also shows plots of classical-quantum sampling results that are discussed in Section IV B.

Theorem 2. Let $\rho_{A^n E} \in \mathcal{S}(A^n E)$ and $1 \leq k \leq n$, let $d = |A|$ be the dimension of a single system, and let $h_2 := \frac{H_2(A^n|E)_\rho}{n}$. Then, we have for $n > d^2$

$$2^{-H_2(A_S|ES)_\rho} = \mathbb{E}_{S \subseteq [n], |S|=k} 2^{-H_2(A_S|E)_\rho} \leq 2^{-kR_d(h_2) + \log(n^2 + 1)}, \quad (15)$$

where $R_d(\cdot)$ is the rate function defined as $R_d(x) := -\log(d - df_d^{-1}(x))$, and $f_d(x) := h(x) + x \log(d^2 - 1) - \log d$.

In terms of smooth min-entropy, we have for any $\varepsilon \in (0, 1]$

$$H_{\min}^\varepsilon(A_S|ES)_\rho \geq kR_d(h_{\min}) - \log(n^2 + 1) - \log \frac{2}{\varepsilon^2}, \quad (16)$$

where $h_{\min} := \frac{H_{\min}(A^n|E)_\rho}{n}$.

See Figure 1 for a plot of $R_2(h_2)$. Note that f_d is an increasing function on $[0, \frac{d^2-1}{d^2}]$ with $f_d(0) = -\log d$ and $f_d(\frac{d^2-1}{d^2}) = \log d$. We can thus define its inverse function $f_d^{-1} : [-\log d, \log d] \rightarrow [0, \frac{d^2-1}{d^2}]$.

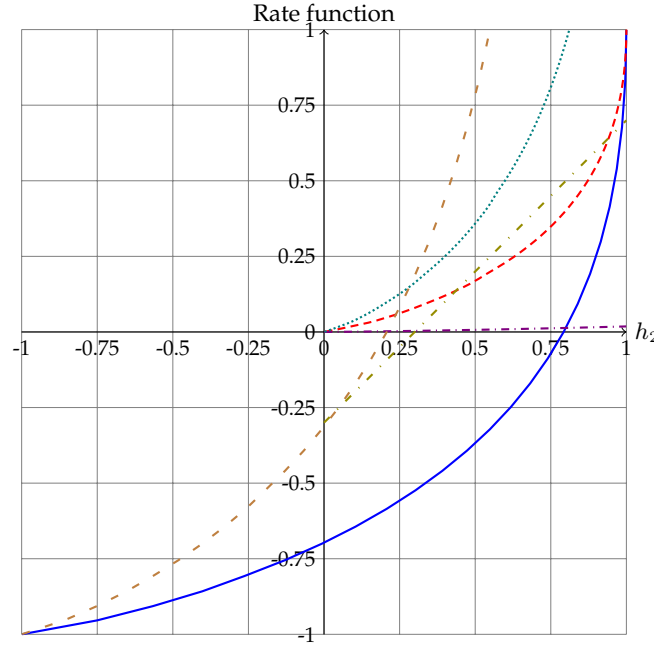


FIG. 1: Plot of our quantum-quantum rate function $R_2(h_2)$ from Theorem 2 (—), our classical-quantum rate function $C_2(h_2)$ from Theorem 6 (---), Wulschleger's min-entropy sampling result [63, Corollary 1] (-.-), Vadhan's purely classical min-entropy sampling results [59, Lemma 6.2] (.....), and the classical and quantum upper bounds we get from a state that is uniform on strings of a fixed type analyzed in Theorems 5 and 8 (....., ---). As Vadhan's result requires a choice of parameters we chose $\tau = 0.1$, which yields a lower bound on the smooth min-entropy, with smoothing parameter of the order of 10^{-6} for a block size of $n = 10000$.

Proof. We start by observing that (15) directly implies (16). This follows from the fact that $h_2 \geq h_{\min}$ (Lemma 17) and Lemma 19.

We now prove (15) by applying Theorem 1 for an appropriately chosen map \mathcal{M} . Define $\mathcal{M}_{A^n \rightarrow A^k S}(X) = \frac{1}{\sqrt{\binom{n}{k}}} \sum_{S \subseteq [n], |S|=k} \text{Tr}_{S^c}[X] \otimes |S\rangle\langle S|$, for $X \in \mathcal{L}(A^n)$, where the second register contains a classical description of the set S , and S^c denotes the complement of S in $[n]$. The reason for this normalization will be clear in the following calculation. Our first task is to relate this map to the task of sampling entanglement. We have

$$\begin{aligned} 2^{-H_2(A^k S|E)_{\mathcal{M}(\rho)}} &= \text{Tr} \left[\left(\rho_E^{-1/4} (\mathcal{M} \otimes \text{id})(\rho_{A^n E}) \rho_E^{-1/4} \right)^2 \right] \\ &= \text{Tr} \left[\left(\rho_E^{-1/4} \left(\frac{1}{\sqrt{\binom{n}{k}}} \sum_{|S|=k} \rho_{A_S E} \otimes |S\rangle\langle S| \right) \rho_E^{-1/4} \right)^2 \right] \\ &= \mathbb{E}_{S \subseteq [n], |S|=k} \text{Tr} \left[\left(\rho_E^{-1/4} \rho_{A_S E} \rho_E^{-1/4} \right)^2 \right] = 2^{-H_2(A_S|ES)_\rho}, \end{aligned}$$

where for the last equality we used the expression for the entropy conditioned on the classical system S (Lemma 23). Note that in the second line above, we slightly abused notation and identified A^k with the spaces A_S for different values of S .

Our second task is to show that our choice of map satisfies the conditions of Theorem 1. We have

$$\begin{aligned} ((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) &= \mathcal{M}^\dagger \left(\frac{1}{\sqrt{\binom{n}{k}}} \sum_{|S|=k} |S\rangle\langle S| \otimes \Phi_{A_S \bar{A}_S} \otimes \text{id}_{\bar{A}_{S^c}} \right) \\ &= \frac{1}{\binom{n}{k}} \sum_{|S|=k} \Phi_{A_S \bar{A}_S} \otimes \text{id}_{A_{S^c} \bar{A}_{S^c}}. \end{aligned}$$

We now write this operator in terms of $\{\Phi_s\}_{s \in [d^2]^n}$. Recall that $\{\frac{1}{\sqrt{d^n}}|\Phi_s\rangle\}_s$ forms an orthonormal basis and thus $\text{id}_{A^n \bar{A}^n} = \frac{1}{d^n} \sum_{s \in [d^2]^n} \Phi_s$:

$$\begin{aligned} ((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) &= \frac{1}{d^{n-k} \binom{n}{k}} \sum_{|S|=k} \sum_{s: \text{supp}(s) \subseteq S^c} \Phi_s \\ &= \frac{1}{d^{n-k} \binom{n}{k}} \sum_{s: |s| \leq n-k} \binom{n-|s|}{k} \Phi_s. \end{aligned}$$

As a result, the coefficients λ_s from Theorem 1 are $\lambda_s = \frac{\binom{n-|s|}{k}}{d^{n-k} \binom{n}{k}}$. Observe that λ_s only depends on $|s|$ and is a decreasing function of $|s|$. In order to apply Theorem 1, it is natural to choose the partition $\mathfrak{S}_+ \cup \mathfrak{S}_-$ of the form $\mathfrak{S}_+ = \{s \in [d^2]^n : |s| \leq \ell_0\}$ and $\mathfrak{S}_- = \{s \in [d^2]^n : |s| > \ell_0\}$ for a value of $\ell_0 \in \{0, \dots, n\}$ to be chosen as a function of h_2 .

Writing equation (11) in our case we obtain,

$$\begin{aligned} 2^{-H_2(A_S|ES)_\rho} &\leq \sum_{\ell=0}^{\ell_0} \frac{\binom{n-\ell}{k}}{d^{n-k} \binom{n}{k}} \binom{n}{\ell} (d^2 - 1)^\ell 2^{-h_2 n} + \frac{\binom{n-\ell_0-1}{k}}{\binom{n}{k}} d^k \\ &= \frac{2^{-h_2 n}}{d^{n-k}} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2 - 1)^\ell + \frac{\binom{n-\ell_0-1}{k}}{\binom{n}{k}} d^k. \end{aligned} \tag{17}$$

Now all that remains is to optimize over ℓ_0 and to find a simple expression for this quantity. Before choosing ℓ_0 , we simplify the expression above. For the second term, we bound

$$\frac{\binom{n-\ell_0-1}{k}}{\binom{n}{k}} d^k \leq \left(\frac{n-\ell_0-1}{n} \right)^k d^k.$$

To obtain a simple bound on the first term, we use the following lemma, which is proven in the appendix.

Lemma 3. For any $\ell_0 \in \{0, \dots, n\}$ such that $\ell_0 \leq \frac{d^2-1}{d^2}n$ where $d^2 < n$, we have

$$\sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell \leq n^2 \binom{n}{\ell_0} (d^2-1)^{\ell_0} \max\left(\frac{n-\ell_0-1}{n}, \frac{1}{d^2}\right)^k.$$

It then follows from equation (17) that

$$2^{-H_2(A_S|ES)_\rho} \leq \max\left(\frac{n-\ell_0-1}{n}, \frac{1}{d^2}\right)^k d^k \left(\frac{2^{-h_2 n}}{d^n} n^2 \binom{n}{\ell_0} (d^2-1)^{\ell_0} + 1\right).$$

We now determine the value of ℓ_0 as a function of h_2 . Observe that using Lemma 25, we have $\binom{n}{\ell} (d^2-1)^\ell \leq 2^{nh(\ell_0/n)} (d^2-1)^{\ell_0} = 2^{nf_d(\ell_0/n)} d^n$ provided $\ell_0 \leq \frac{d^2-1}{d^2}n$. We define ℓ_0 to be the largest integer that is at most $\frac{d^2-1}{d^2}n$ such that $f_d(\ell_0/n) \leq h_2$. As a result, we have

$$2^{-H_2(A_S|ES)_\rho} \leq \max\left(\frac{n-\ell_0-1}{n}, \frac{1}{d^2}\right)^k d^k (n^2 + 1). \quad (18)$$

Observe also that in the case where the maximum is $1/d^2$, the result follows directly as $R_d(h_2) \leq \log d$. In the case where $(n-\ell_0-1)/n > 1/d^2$, we observe that $(\ell_0+1)/n > f_d^{-1}(h_2)$ by our choice of ℓ_0 . Note that if $\ell_0+1 \leq (d^2-1)/d^2 \cdot n$, this follows from the fact that f_d is nondecreasing, and otherwise it follows from the fact that by definition f_d^{-1} is always upper bounded by $(d^2-1)/d^2$.

We now write $\left(\frac{n-\ell_0-1}{n}\right)^k$ in terms of the entropy rate h_2 :

$$\begin{aligned} k \log\left(\frac{n-\ell_0-1}{n}\right) &= k \log\left(1 - \frac{\ell_0+1}{n}\right) \\ &\leq k \log(1 - f_d^{-1}(h_2)) \\ &= k \log(d - df_d^{-1}(h_2)) - k \log d \\ &= -kR_d(h_2) - k \log d. \end{aligned}$$

By plugging these inequalities into (18), we obtain the desired result. \square

2. An upper bound on the rate function

Note that the rate function obtained in Theorem 2 is independent of the state ρ_{AE} and of the size of the sample k . The objective of this section is to show that with such a requirement, the rate function R_d cannot be improved too much especially when h_2 is close to the minimal value of $-\log d$.

Definition 4. We define the optimal rate function R_d^{opt} as

$$R_d^{\text{opt}}(h_2) := \liminf_{n \geq 1} \left(\min_{k \in [n], \rho_{A^n E} \text{ such that } \frac{1}{n} H_2(A^n|E) \geq h_2} \frac{1}{k} H_2(A_S|ES)_\rho \right),$$

where $A^n = A_1, \dots, A_n$ is comprised of n qudits of dimension d .

We now derive an upper bound on the rate function that will show that our result is fairly close to optimal for small h_2 and small k . The idea is to choose a state that consists of n EPR pairs that have been corrupted by a fixed-weight generalized Pauli error. In this case, if this weight is small enough, the sample will avoid all the errors with relatively large probability and the collision entropy of the sampling is going to be much smaller than kh_2 .

Theorem 5. It holds that $R_d^{\text{opt}}(h_2) \leq -\log(d - 2df_d^{-1}(h_2))$.

Proof. Let $E = B^n \cong A^n$, and consider the state

$$\rho_{A^n B^n} = \left(\binom{n}{w} (d^2-1)^w \right)^{-1} \sum_{s, |s|=w} \frac{\Phi_s}{d^n}$$

for some particular w . This is a maximally entangled state between A^n and B^n that has been corrupted by a random error of weight exactly w . We can compute its collision entropy

$$\begin{aligned} 2^{-H_2(A^n|B^n)_\rho} &= \text{Tr}[\rho_{B^n}^{-1/2} \rho_{A^n B^n} \rho_{B^n}^{-1/2} \rho_{A^n B^n}] = \left(\binom{n}{w} (d^2 - 1)^w \right)^{-2} \sum_{s, |s|=w} \text{Tr}[\text{id}_{A^n}] \\ &= \left(\binom{n}{w} (d^2 - 1)^w \right)^{-1} d^n \\ &\leq 2^{-nh(w/n) - w \log(d^2 - 1) + n \log d + \log n}. \end{aligned}$$

Hence, $h_2 \geq f_d(w/n) - \frac{1}{n} \log n$.

Now, let us compute the collision entropy for a random subsystem of size k with $\frac{k}{n} \rightarrow 0$. Note that we have

$$\rho_{A_S B^n} = \sum_{s \in [d^2]^S} \mathbf{Pr}\{\sigma_S = s\} \frac{\Phi_s \otimes \text{id}_{B_S^c}}{d^n},$$

where $\sigma \in [d^2]^n$ is a random string of weight exactly w , and σ_S is the substring index by elements of S . Then we have

$$\begin{aligned} \text{Tr} \left[\left(\rho_{B^n}^{-1/4} \rho_{A_S B^n} \rho_{B^n}^{-1/4} \right)^2 \right] &= \sum_{s, s' \in [d^2]^S} \mathbf{Pr}\{\sigma_S = s\} \mathbf{Pr}\{\sigma'_S = s'\} \frac{\text{Tr}[\Phi_s \Phi_{s'}]}{d^k} \\ &= d^k \mathbf{Pr}\{\sigma_S = \sigma'_S\}. \end{aligned}$$

Thus, we want to evaluate the average over S of this probability. For any fixed σ and σ' of weight w and choosing a random subset of size k , the corresponding substrings will be the same if they avoid all positions where σ or σ' are non-zero. As a result the collision probability for the sample is at least

$$\begin{aligned} \frac{n-2w}{n} \cdots \frac{n-2w-k+1}{n-k+1} &\geq \left(\frac{n-k-2w}{n-k} \right)^k \\ &= \left(1 - 2 \left(\frac{w}{n} \right) \left(\frac{n}{n-k} \right) \right)^k \\ &\geq \left(1 - 2f_d^{-1} \left(h_2 + \frac{1}{n} \log n \right) \left(\frac{n}{n-k} \right) \right)^k. \end{aligned}$$

Taking the limit over $n \rightarrow \infty$ and $\frac{k}{n} \rightarrow 0$, we get that

$$2^{-H_2(A_S|E)} \geq (d(1 - 2f_d^{-1}(h_2)))^k.$$

This directly yields the theorem. \square

3. Applications of entanglement sampling

An immediate consequence of our result on entanglement sampling concerns the existence of decouplers (QQ-extractors) using only very few qubits. A decoupling operation is some process $\mathcal{K}_{A \rightarrow B}$ that applied to the A system transforms ρ_{AE} to a state that is close to $\tau_B \otimes \rho_E$, where τ_B is a state that depends only on the map \mathcal{K} but not on the initial state ρ_{AE} . In quantum information theory, such processes typically consist of applying a random unitary U to A , followed by a map $\mathcal{T}_{A \rightarrow B}$ such as the partial trace operation. That is, the map \mathcal{K} is of the form $\mathcal{K}(\rho_A) = \int d\mu(U) \mathcal{T}_{A \rightarrow B}(U \rho_A U^\dagger) \otimes |U\rangle\langle U|$, where $|U\rangle$ is a classical register containing the choice of unitary.

Decoupling theorems in quantum information theory have their origin in quantum channel coding [1, 30, 32] where \mathcal{T} is usually the partial trace, and $\tau_B = \text{id}/|B|$. In this context, the size of the system $|B|$ that one can decouple from E , can be related to the number of qubits that one can pass through a quantum channel whose environment is E with vanishing error. In this context, the choice of unitary U yields an encoding scheme (see [24] for details). More recently, the decoupling theorem has been generalized to a wide variety of maps \mathcal{T} [24, 25].

Decoupling results are known when the unitaries are chosen from the Haar measure [1, 24, 25, 30], from a 2-design, from an approximate 2-design [52], or from even more efficient sets of unitaries [13]. In contrast, when A is classical,

many decoupling operations are known in the form of randomness extractors discussed in the introduction (see [58] for a survey). Of particular interest in both computational [30] and physical applications [22, 23, 31, 33] are unitaries which are efficient. In a computational setting, this generally refers to unitaries that can be implemented using low-depth quantum circuits, whereas in physical scenarios it is usually of interest that they arise from Hamiltonians involving only nearest neighbour interactions over a short period of time.

As an example of the physical relevance of decoupling theorems, let us consider the case where A is comprised of a system A_{sys} and a bath A_{bath} , and $\mathcal{T} = \text{Tr}_{A_{\text{bath}}}$ is the operation that traces out the bath. A decoupling theorem for certain classes of unitaries then says that for very many unitaries in that set, the resulting state of the system τ_B is independent of its initial state, one of the steps considered in the process of thermalization [39]. That is, it tells us that certain evolutions of the system and the bath, namely those corresponding to such unitaries, can lead to thermalization. This holds even in the stronger sense of relative thermalization where one requires that the state of the system becomes independent of an observer holding E [23]. In fact, the decoupling theorem [25] for Haar measure random unitaries can even be used [33] to recover the results of [48] stating that for most initial states of A , or equivalently most unitary evolutions on A , the resulting state is close to the canonical state.

As such, it is an interesting question to determine which sets of unitaries lead to a decoupling theorem. Here, our goal is to show that if $A^n = A_1, \dots, A_n$ consists of n qudits, then there exist decoupling operations involving only a (small) subset of such qudits. As outlined in the introduction, one generic way to accomplish this task is to show that the fully quantum min-entropy can be sampled. Decoupling operations involving only few qudits can then be obtained in a “sample-then-decouple” fashion similar to the classical “sample-then-extract” approach of [59]. That is, one first samples a set of qubits, and then applies an arbitrary decoupling operation on the resulting sample.

Our result extends to any of the more modern decoupling theorems involving entropy measures [24, 25].⁴ To illustrate this idea, let us consider the example of $A^n = A_1, \dots, A_n$ consisting of n qubits, unitaries chosen from the Haar measure, and \mathcal{T} being the partial trace operation $\text{Tr}_{n-r}(\rho_A)$ tracing out all but r of the n qubits. In terms of the H_2 entropy it was shown [24, 25] that

$$\int d(U) \left\| \text{Tr}_{n-r} \otimes \text{id}_E(\rho_{AE}) - \frac{\text{id}}{2^r} \otimes \rho_E \right\|_1 \leq 2^{-\frac{1}{2}(H_2(A|E) + n - 2r)}, \quad (19)$$

where $\|\rho - \sigma\|_1$ is the trace distance of ρ and σ . If we now first sample a subset of size k of the qubits, then our sampling result states that for unitaries chosen according to the Haar measure of qubits

$$\int d(U) \left\| \text{Tr}_{|S|-r} \otimes \text{id}_E(\rho_{AES}) - \frac{\text{id}}{2^r} \otimes \rho_{ES} \right\|_1 \leq 2^{-\frac{1}{2} \left[|S| \left(R_2 \left(\frac{H_2(A|E)}{n} \right) - 1 \right) - 2r - \log(n^2 + 1) \right]}, \quad (20)$$

for the rate function given in Theorem 2. Similarly, our sampling result can be applied to the special kinds of decoupling maps known as quantum-to-classical randomness extractors [11]. In this context, sampling allows the generation of classical randomness from a quantum system⁵ by applying measurements to only a few of the qubits of A .

B. Classical-quantum min-entropy sampling

1. Statement

Observe that in the case where the system A^n is classical, i.e., $\rho_{A^n E} = \sum_{x^n \in [d]^n} p(x^n) |x^n\rangle\langle x^n| \otimes \rho_E(x^n)$ for some distribution p and states $\rho_E(x^n)$, Theorem 2 can still be applied but in many cases it give trivial bounds. In fact, when A^n is classical, we have $H_2(A^n|E) \geq 0$ as well as $H_2(A_S|ES) \geq 0$. In order to improve on the lower bound of Theorem 2 in the case of a classical system, we can apply Theorem 1 to a more specific map \mathcal{M} that *measures* the systems A_S that are sampled. This allows us to obtain a lower bound on the collision entropy $H_2(A_S|ES)$ that is nontrivial for the entire range $H_2(A^n|E) \in [0, n \log d]$.

Unlike the fully quantum case about which not much was known, the classical-quantum min-entropy sampling has been previously studied in particular in [6, 38, 63]. We briefly highlight the similarities and differences with our results in Theorem 6. The work of [6] is restricted to the case where A^n is uniformly distributed and obtains

⁴ In contrast to statements involving only the dimensions of systems as in e.g., [1].

⁵ Of which we only have a guarantee about the entropy.

a lower bound on the non-smoothed min-entropy⁶ of the sample as a function of the dimension of the system E rather than the conditional entropy. This special case is particularly interesting in the context of random access codes. The parameters they obtain are better when the dimension of E is small, i.e., h_2 is large. However, their techniques fail to give a nontrivial bound when h_2 is small. See Section IV C for more details. The sampling theorem of [63] works for general classical-quantum states and gives a lower bound on the non-smoothed min-entropy of the sample. The parameters are illustrated in Figure 1. The work of [38] considers the general classical-quantum case and focuses on the smoothed min-entropy. This result extends Vadhan's classical min-entropy sampling [59] result to the case of quantum side information. Hiding technicalities (like the fact one should sample blocks rather than bits) and neglecting terms that depend on the smoothing parameters, the rate function they obtain is basically optimal $R(\alpha) = \alpha$,⁷ as the plot of Vadhan's result in Figure 1.

Our sampling result has an application to randomness extraction, in that it yields a general way to construct locally computable extractors even with respect to quantum side information E . This is analogous to the application of entanglement sampling to decoupling discussed above.

Theorem 6. *Let $\rho_{A^n E}$ be a classical-quantum state, and $1 \leq k \leq n$, let $d = |A|$, and let $h_2 := \frac{H_2(A^n|E)_\rho}{n}$. Then, for any $n > d$,*

$$2^{-H_2(A_S|ES)_\rho} = \mathbb{E}_{S \subseteq [n], |S|=k} 2^{-H_2(A_S|E)_\rho} \leq 2^{-kC_d(h_2) + \log(n^2+1)},$$

where $C_d(\cdot)$ is the rate function defined as $C_d(\alpha) := -\log(1 - c_d^{-1}(\alpha))$, and $c_d(\alpha) := h(\alpha) + \alpha \log(d-1)$. In terms of smooth min-entropy, we have for any $\varepsilon \in (0, 1]$

$$H_{\min}^\varepsilon(A_S|ES)_\rho \geq kC_d(h_{\min}) - \log(n^2+1) - \log \frac{2}{\varepsilon^2}, \quad (21)$$

where $h_{\min} := \frac{H_{\min}(A^n|E)_\rho}{n}$.

See Figure 1 for a plot of $C_2(h_2)$. Note that c_d is an increasing function on $[0, \frac{d-1}{d}]$ with $c_d(0) = 0$ and $c_d(\frac{d-1}{d}) = \log d$. The inverse function $c_d^{-1} : [0, \log d] \rightarrow [0, \frac{d-1}{d}]$ is therefore well-defined.

Proof. The proof is very similar to that of Theorem 2: one uses Theorem 1 with $\mathcal{M}_{A^n \rightarrow A^k S}(X) = \frac{1}{\sqrt{\binom{n}{k}}} \sum_{S \subseteq [n], |S|=k} \sum_{x^k \in [d]^S} \langle x^k | \text{Tr}_{S^c}[X] | x^k \rangle \otimes |x^k\rangle \langle x^k| \otimes |S\rangle \langle S|$, where $\{|x^k\rangle\}_{x^k \in [d]^S}$ is the standard basis of A_S . We then find that

$$((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) = \frac{1}{\binom{n}{k}} \sum_{|S|=k} \left(\sum_{x^k} |x^k\rangle \langle x^k|_{A_S} \otimes |x^k\rangle \langle x^k|_{\bar{A}_S} \right) \otimes \text{id}_{A_{S^c} \bar{A}_{S^c}}.$$

Recall that we want to write this operator in terms of $\Phi_s = (W_s \otimes \text{id})\Phi_{A^n \bar{A}^n}(W_s^\dagger \otimes \text{id})$, where $W_s = W_{s_1} \otimes \cdots \otimes W_{s_n}$ is a product of generalized Pauli operators. Let us now assume that the numbering of the Pauli operators is such that W_0, \dots, W_{d-1} are defined as $W_y|x\rangle = e^{2\pi i xy/d}|x\rangle$ for all $x, y \in [d]$. It then follows that

$$\begin{aligned} \frac{1}{d} \sum_{y \in [d]} \Phi_y &= \frac{1}{d} \sum_{y \in [d]} \sum_{x, x' \in [d]} e^{2\pi i (x-x')y/d} |x\rangle \langle x'| \otimes |x\rangle \langle x'| \\ &= \sum_x |x\rangle \langle x|_A \otimes |x\rangle \langle x|_{\bar{A}}. \end{aligned}$$

As a result, we can write

$$\begin{aligned} ((\mathcal{M}^\dagger \circ \mathcal{M}) \otimes \text{id}_{\bar{A}^n})(\Phi_{A^n \bar{A}^n}) &= \frac{1}{\binom{n}{k} d^n} \sum_{|S|=k} \sum_{\substack{s \in [d^2]^n \\ s_i \in [d], i \in S}} \Phi_s \\ &= \frac{1}{\binom{n}{k} d^n} \sum_{s: |s| < d \leq n-k} \binom{n-|s|}{k} \Phi_s, \end{aligned}$$

⁶ The fact that the min-entropy is non-smoothed is important for the application to random access codes.

⁷ To obtain such a result, smoothing is in fact necessary as shown by the example of Theorem 8.

where $|s|_{<d} = |\{i \in [n] : s_i \in [d]\}|$. As a result, the coefficients λ_s from Theorem 1 are $\lambda_s = \frac{\binom{n-|s|_{<d}}{k}}{d^n \binom{n}{k}}$, which only depends on $|s|_{<d}$ and is a decreasing function of $|s|_{<d}$. As before, it is natural to choose the partition $\mathfrak{S}_+ \cup \mathfrak{S}_-$ from Theorem 1 of the form $\mathfrak{S}_+ = \{s \in [d^2]^n : |s|_{<d} \leq \ell_0\}$ and $\mathfrak{S}_- = \{s \in [d^2]^n : |s|_{<d} > \ell_0\}$ for a value of $\ell_0 \in \{0, \dots, n\}$ to be chosen as a function of h_2 . We then have

$$\begin{aligned} 2^{-H_2(A_S|ES)_\rho} &\leq \sum_{\ell=0}^{\ell_0} \frac{\binom{n-\ell}{k}}{d^n \binom{n}{k}} \binom{n}{\ell} (d^2 - d)^\ell d^{n-\ell} 2^{-h_2 n} + \frac{\binom{n-\ell_0-1}{k}}{\binom{n}{k}} \\ &\leq 2^{-h_2 n} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d-1)^\ell + \left(\frac{n-\ell_0-1}{n} \right)^k. \end{aligned} \quad (22)$$

To obtain a simple bound on the first term, we use the same Lemma 3 as in the proof of Theorem 2 replacing d^2 by d . Equation (22) then becomes

$$2^{-H_2(A_S|ES)_\rho} \leq \max \left(\frac{n-\ell_0-1}{n}, \frac{1}{d} \right)^k \left(2^{-h_2 n} n^2 \binom{n}{\ell_0} (d-1)^{\ell_0} + 1 \right).$$

We now determine the value of ℓ_0 as a function of h_2 . Observe that using Lemma 25, we have $\binom{n}{\ell_0} (d^2 - 1)^{\ell_0} \leq 2^{nh(\ell_0/n)} (d-1)^{\ell_0} = 2^{nc_d(\ell_0/n)}$ provided $\ell_0 \leq \frac{d-1}{d}n$. We define ℓ_0 to be the largest integer that is at most $\frac{d-1}{d}n$ such that $c_d(\ell_0/n) \leq h_2$. As a result, we have

$$2^{-H_2(A_S|ES)_\rho} \leq \max \left(\frac{n-\ell_0-1}{n}, \frac{1}{d} \right)^k (n^2 + 1). \quad (23)$$

If the maximum is $1/d$, then we directly get the desired result. Now we use the maximality of ℓ_0 to say that $(\ell_0 + 1)/n > c_d^{-1}(h_2)$. Finally,

$$\begin{aligned} k \log \left(\frac{n-\ell_0-1}{n} \right) &= k \log \left(1 - \frac{\ell_0+1}{n} \right) \\ &\leq k \log(1 - c_d^{-1}(h_2)) \\ &= -kC_d(h_2). \end{aligned}$$

By plugging these inequalities into (23), we obtain the desired result. \square

2. An upper bound on the classical rate function

Like in the quantum case, one can find an upper bound for the rate function. Here, our upper bound will even hold for non-conditional entropy (i.e., when E is trivial).

Definition 7. We define the optimal classical rate function C_d^{opt} as

$$C_d^{\text{opt}}(h_2) := \liminf_{n \geq 1} \left(\min_{k \in [n], \rho_{X^n|E} \text{ such that } \frac{1}{n} H_2(X^n|E) \geq h_2} \frac{1}{k} H_2(X_S|ES)_\rho \right),$$

where $X^n = X_1, \dots, X_n$ is comprised of n dits of dimension d .

We will now derive an upper bound on the rate function that will show that our result is fairly close to optimal for small h_2 and small k . We will derive our upper bound by considering the uniform distribution over strings of fixed Hamming weight. As in the fully quantum case, it will turn out that distributions of small Hamming weight still have a relatively high h_2 compared to the probability of getting a 0 in the sample, and this yields an average entropy for the sample that is much lower than kh_2 .

Theorem 8. It holds that $C_d^{\text{opt}}(h_2) \leq -\log(1 - 2c_d^{-1}(h_2))$.

Proof. Let E be trivial, and consider the state

$$\rho_{X^n} = |\{s, |s| = w\}|^{-1} \sum_{s, |s|=w} |s\rangle\langle s|$$

for some particular w . We can compute its collision entropy:

$$\begin{aligned} \text{Tr}[\rho_{X^n}^2] &= |\{s, |s| = w\}|^{-1} \\ &= \binom{n}{w}^{-1} (d-1)^{-w} \\ &\leq 2^{-nh(w/n) - w \log(d-1) + \log n}. \end{aligned}$$

Hence, $h_2 \geq c_d(w/n) - \frac{1}{n} \log n$.

Now, let us compute the collision entropy of the sample when $\frac{k}{n} \rightarrow 0$. Fix a pair of strings s and s' with weight w . Choosing a random subset of size k , the corresponding substrings will be the same if they avoid all positions where s or s' are non-zero. As a result the collision probability for the sampled substring is at least

$$\begin{aligned} \frac{n-2w}{n} \cdots \frac{n-2w-k+1}{n-k+1} &\geq \left(\frac{n-k-2w}{n-k} \right)^k \\ &= \left(1 - 2 \left(\frac{w}{n} \right) \left(\frac{n}{n-k} \right) \right)^k \\ &\geq \left(1 - 2c_d^{-1} \left(h_2 + \frac{1}{n} \log n \right) \left(\frac{n}{n-k} \right) \right)^k. \end{aligned}$$

Taking the limit over $n \rightarrow \infty$ and $\frac{k}{n} \rightarrow 0$, we get that

$$2^{-H_2(A_S|E)} \geq (1 - 2c_d^{-1}(h_2))^k.$$

This directly yields the theorem. □

C. Dimension bounds for random access codes

One application of our sampling results is to bound the dimension of quantum random access codes. To translate a result about min-entropy sampling into a result concerning random access codes, one simply considers the system E to be composed of m bits or qubits and then considers the special case of a uniform distribution on $X_1 \dots X_n$. That is, the state $\rho_{X^n E}$ is of the form

$$\rho_{X^n E} = \frac{1}{2^n} \sum_{x^n \in \{0,1\}^n} |x^n\rangle\langle x^n| \otimes \rho_E^{x^n}. \quad (24)$$

The quantity of interest when studying a random access encoding of a classical string X^n is the minimal dimension of E needed to recover any subset of size k of the bits with some desired probability p . Recall the operational interpretation of the conditional min-entropy $H_{\min}(X_S|ES)$ as the best probability for guessing the bitstring X_S when having access to the system E . Thus, a lower bound on the min-entropy $H_{\min}(X_S|ES)$ directly gives an upper bound on the probability of successfully recovering a randomly chosen system S of size k . The latter is exactly the success probability of k -out-of- n random access code as defined in [6].

More precisely, using Lemma 18, Theorem 6 directly leads to a lower bound on the success probability p of k -out-of- n using m qubits $p \leq \sqrt{2^{-kC_d(1-m/n)+\log(n^2+1)}}$. Compared to [6], this bound is better when m is close to n . Specifically, when $m/n > 0.721$, the technique of [6] does not give any probability bound. On the other hand, when m/n becomes smaller, their probability bound becomes smaller. k -out-of- n random access codes have also been studied in [63] and nontrivial upper bounds on the success probabilities are obtained for all values of m . The exponent of the success probability is illustrated in Figure 1 (note that the plot for C_d should be divided by two to interpret it as a guessing probability).

One could similarly define fully quantum random access codes. In this setting, we want to store n qudits A_1, \dots, A_n of information into m qudits so that a subset of k qudits chosen at random can be recovered. Given n and m , one can define the maximum average fidelity $F_{n,m,k}$ with which k qudits can be recovered. As before, our goal will be to bound the dimension necessary to achieve a desired fidelity, or equivalently, establish an upper bound on the achievable fidelity as a function of the dimension.

Theorem 9. *Let $n > d^2$. For any $m \leq n$ and $1 \leq k \leq n$*

$$F_{n,m,k}^2 \leq 2^{-\frac{1}{2}k(R_d(-\frac{m}{n}\log d) + \log d) + \frac{1}{2}\log(n^2+1)}$$

Proof. Let A^n be the system containing the n qudits to be stored and E be the m qudits of storage. Then, for any $\rho_{A^n E}$, we have $H_2(A^n|E) \geq -m \log d$. Using Theorem 2 and Lemma 17, we have

$$\begin{aligned} 2^{-H_{\min}(A_S|ES)\sigma} &= \mathbb{E}_{S \subseteq [n], |S|=k} 2^{-H_{\min}(A_S|E)\rho} \\ &\leq \mathbb{E}_{S \subseteq [n], |S|=k} 2^{-\frac{1}{2}(H_2(A_S|E)\rho - k \log d)} \\ &\leq 2^{-\frac{1}{2}(kR_d(-\frac{m}{n}\log d) - \log(n^2+1) - k \log d)} \\ &\leq 2^{-\frac{1}{2}k(R_d(-\frac{m}{n}\log d) - \log d) + \frac{1}{2}\log(n^2+1)}, \end{aligned}$$

where $\sigma_{A^n ES} = \rho_{A^n E} \otimes \binom{\text{id}_S}{n}$, with S representing the choice of subset of k qudits we want to recover. Now observe that $2^{-H_{\min}(A_S|ES)} = 2^{k \log d} \max_{\mathcal{E}_{ES} \rightarrow A'_S} F(\Phi_{A_S A'_S}^N, \text{id}_{A_S} \otimes \mathcal{E}(\rho_{ES}))^2$. The fidelity term is exactly the maximum fidelity with which the state on A_S can be recovered from the system E . \square

D. High-order uncertainty relations against quantum side-information

Uncertainty relations play a fundamental role in quantum information and in particular in quantum cryptography. Many of the modern security proofs for quantum key distribution are based on an uncertainty relation [9, 56, 57]. They are also at the heart of security proofs in the bounded quantum storage model [11, 18, 19]. An uncertainty relation is a statement about a guaranteed uncertainty in the outcome of a measurement in a randomly chosen basis. We refer the reader to [61] for a survey on uncertainty relations.

1. Uncertainty relation for BB84 measurements

Specifically, here we consider a system A^n of n qubits. Then we measure each one of these qubits in either the standard basis (labeled 0 with vector $|0\rangle, |1\rangle$) or the Hadamard basis (labeled 1 with vectors $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$). More precisely, choose a random vector $\Theta^n \in \{0, 1\}^n$ and measure qubit i in the basis specified by the i -th component of $\Theta^n = \Theta_1, \dots, \Theta_n$. Call the outcome X_i . An uncertainty relation is a statement about the amount of uncertainty in the random variable $X^n = X_1, \dots, X_n$ given the knowledge of the basis choice Θ^n . The uncertainty is often measured in terms of the Shannon entropy. However, for the applications we consider here, the measure of uncertainty needs to be stronger, i.e., we should use a higher order entropy like H_{\min} or H_2 . Such an uncertainty relation has been established in [18]:

$$H_{\min}^\varepsilon(X^n|\Theta^n) \gtrsim n/2. \quad (25)$$

The way this uncertainty relation was used in the context of the bounded storage model was to apply a chain rule to (25) to obtain $H_{\min}^\varepsilon(X^n|E\Theta^n) \gtrsim n/2 - \log|E|$. There are two reasons for this inequality to be unsatisfactory: it depends on the dimension of E rather than on the correlations between A^n and E , and it becomes trivial when $H_2(A^n|E) < -n/2$ as this implies $\log|E| > n/2$.

It is simple to see that if the system A^n is maximally entangled with some system E , then the outcome X^n of this measurement can be perfectly predicted by having access to E . In other words, if the conditional entropy $H_2(A^n|E) = -n$, then X^n can be correctly guessed with probability 1. The following theorem provides a converse: if $H_2(A^n|E) \geq -(1 - \varepsilon)n$ for $\varepsilon > 0$, then X^n cannot be guessed with probability better than $2^{-n\delta(\varepsilon)}$ with $\delta(\varepsilon) > 0$ whenever $\varepsilon > 0$.

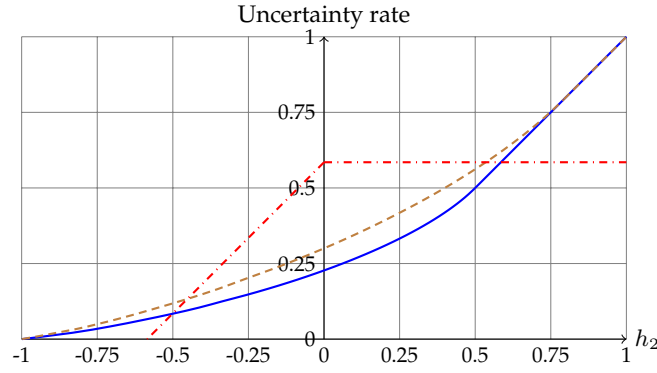


FIG. 2: Plot of the function $\gamma(h_2)$ (—) from Theorem 10 giving a lower bound on the uncertainty of the outcome of BB84 measurement as a function of the entropy rate h_2 of the state being measured. For measurements in the six-state bases, the uncertainty rate function we obtain in Theorem 12 is $\gamma_2(h_2)$ (---). For comparison, we also plot the uncertainty rate function proved in [11] (-.-.).

Theorem 10. Let $\rho_{A^n E} \in \mathcal{S}(A^n E)$ where A^n is an n -qubit space and define $h_2 = \frac{H_2(A^n|E)_\rho}{n}$. Then we have

$$H_2(X^n|E\Theta^n)_\rho \geq n\gamma(h_2) - 1$$

where $\rho_{X^n E\Theta^n} = \frac{1}{2^n} \sum_{x^n \in \{0,1\}^n, \theta^n \in \{0,1\}^n} |x^n\rangle\langle x^n| \langle x^n| H^{\theta^n} \rho_{A^n E} H^{\theta^n} |x^n\rangle \otimes |\theta^n\rangle\langle \theta^n|$ is the state obtained when system A^n is measured in the basis defined in the register Θ^n and the function γ is defined by

$$\gamma(h_2) = \begin{cases} h_2 & \text{if } h_2 \geq 1/2 \\ g^{-1}(h_2) & \text{if } h_2 < 1/2. \end{cases}$$

with $g(\alpha) = h(\alpha) + \alpha - 1$.

Proof. We apply Theorem 1 with $\mathcal{M}_{A^n \rightarrow X^n \Theta^n} = \mathcal{N}^{\otimes n}$ where $\mathcal{N}(\rho) = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}, \theta \in \{0,1\}} |\theta\rangle\langle \theta| \otimes |x\rangle\langle x| \langle x| H^\theta \rho H^\theta |x\rangle$. We have

$$\begin{aligned} 2^{-H_2(X^n \Theta^n | E)_{\mathcal{M}(\rho)}} &= \text{Tr} \left[\left(\rho_E^{-1/4} (\mathcal{N}^{\otimes n} \otimes \text{id}) (\rho_{A^n E}) \rho_E^{-1/4} \right)^2 \right] \\ &= \frac{1}{2^n} \sum_{\theta^n \in \{0,1\}^n} \text{Tr} \left[\left(\rho_E^{-1/4} \sum_{x^n \in \{0,1\}^n} |\theta^n\rangle\langle \theta^n| \otimes |x^n\rangle\langle x^n| \langle x^n| H^{\theta^n} \rho_{A^n E} H^{\theta^n} |x^n\rangle \rho_E^{-1/4} \right)^2 \right] \\ &= 2^{-H_2(X^n | E\Theta^n)_\rho}, \end{aligned}$$

where in the last line we used the expression for the entropy conditioned on a classical system (Lemma 23).

We then evaluate the state

$$\begin{aligned} (\mathcal{N}^\dagger \circ \mathcal{N} \otimes \text{id})(\Phi) &= \frac{1}{2} (|00\rangle\langle 00| + |11\rangle\langle 11| + |++\rangle\langle ++| + |--\rangle\langle --|) \\ &= \frac{1}{2} \left(\Phi_0 + \frac{1}{2}\Phi_1 + \frac{1}{2}\Phi_3 \right), \end{aligned}$$

where Φ_i are defined in Equations (9) and (10).⁸ In the notation of Theorem 1, we have for the map \mathcal{M} and for $s \in \{0, 1, 3\}^n$, $\lambda_s = \frac{1}{2^n} \cdot \frac{1}{2^{|s|}}$. For $s \notin \{0, 1, 3\}^n$, $\lambda_s = 0$. As a result, when applying Theorem 1, it is natural to choose the partition $\mathfrak{S}_+ \cup \mathfrak{S}_-$ of the form $\mathfrak{S}_+ = \{s \in [d^2]^n : |s| \leq \ell_0\}$ and $\mathfrak{S}_- = \{s \in [d^2]^n : |s| > \ell_0\}$ for a value of $\ell_0 \in \{0, \dots, n\}$ to be chosen as a function of h_2 . We obtain for any ℓ_0

$$2^{-H_2(X^n | E\Theta^n)_\rho} \leq \sum_{\ell=0}^{\ell_0} \binom{n}{\ell} 2^{-h_2 n - n} + 2^{-\ell_0 - 1} \delta_{\ell_0 \leq n-1}, \quad (26)$$

⁸ Note that Φ_2 is the projector on the anti-symmetric subspace and hence cannot appear in this decomposition.

where $\delta_{\ell_0 \leq n-1} = 1$ if $\ell_0 \leq n-1$ and 0 if $\ell_0 = n$. If $h_2 \geq 1/2$, let $\ell_0 = n$, in which case we obtain a bound of

$$2^{-H_2(X^n|E\Theta^n)_\rho} \leq 2^{-h_2 n}.$$

If $h_2 < 1/2$, then we are going to choose $\ell_0 \leq n/2$. Define the function $g(\alpha) = h(\alpha) + \alpha - 1$ and let $\alpha_0 \leq 1/2$ be such that $g(\alpha_0) = h_2$. We then choose $\ell_0 = \lfloor \alpha_0 n \rfloor$. As a result,

$$\begin{aligned} \sum_{\ell=0}^{\ell_0} \binom{n}{\ell} 2^{-h_2 n - n} &\leq 2^{n(h(\ell_0/n) - h_2 - 1)} \\ &\leq 2^{n(h(\alpha_0) - h_2 - 1)} = 2^{n(-\alpha_0 + 1 + h_2 - h_2 - 1)} = 2^{-\alpha_0 n}, \end{aligned}$$

where the first inequality is due to Lemma 25. In addition, we have $2^{-\ell_0 - 1} \leq 2^{-\alpha_0 n}$. Using these bounds in (26), we obtain in this case

$$2^{-H_2(X^n|E\Theta^n)_\rho} \leq 2^{-\alpha_0 n + 1}.$$

Taking the logarithm leads to the desired result. \square

The following corollary expresses the uncertainty relation described in Theorem 10 in terms of min-entropies, which will be more convenient for the cryptographic applications.

Corollary 11. *Using the same notation as in Theorem 10, we have*

$$H_{\min}(X^n|E\Theta^n)_\rho \geq \frac{1}{2}(n\gamma(h_2) - 1) \quad (27)$$

$$\geq \frac{1}{2}(n\gamma(h_{\min}) - 1). \quad (28)$$

where $h_{\min} = \frac{H_{\min}(A^n|E)_\rho}{n}$. Moreover, for any $\varepsilon \in (0, 1]$, we have

$$H_{\min}^\varepsilon(X^n|E\Theta^n)_\rho \geq n\gamma(h_2) - 1 - \log \frac{2}{\varepsilon^2}. \quad (29)$$

Proof. To obtain (27), observe that $H_{\min}(X^n|E\Theta^n)_\rho \geq \frac{1}{2}H_2(X^n|E\Theta^n)_\rho$, using Lemma 18. To replace h_2 by h_{\min} , we use the corresponding lower bound in Lemma 17. To obtain (29), we use Lemma 19. \square

2. Uncertainty relation for measurements in MUBs

Consider a system A^n of n qudits and consider a full set of $d+1$ mutually unbiased bases (MUBs) in dimension d . A set of bases are said to be mutually unbiased if for any pair of vectors $|v\rangle, |w\rangle$ in two different bases, we have $|\langle v|w\rangle| = d^{-1/2}$. We then measure each one of these qudits in a randomly chosen basis from this set. More precisely, choose a random vector $\Theta^n \in [d+1]^n$ and measure qudit i in the basis specified by the i -th component of Θ^n . Let U_{θ^n} be the unitary that transforms the basis θ^n into the standard basis. We prove an uncertainty relation for these measurements in the presence of quantum side information. Previously, uncertainty relations for these measurements taking into account possible quantum side information were proven in [11]. The main improvement here is that the uncertainty lower bound is nontrivial for any $h_2 > -\log d$. Specifically, for entropy rates $h_2 < -(\log(d+1) - 1)$, this theorem provides the first nontrivial uncertainty rates for single-qudit measurements in MUBs. However, when h_2 is close to 0, the bound of [11] is better than the one provided here. See Figure 2 for a comparison.

Theorem 12. *Let $\rho_{A^n E} \in \mathcal{S}(A^n E)$ where A^n is an n -qudit space and define $h_2 = \frac{H_2(A^n|E)_\rho}{n}$. Then we have*

$$H_2(X^n|E\Theta^n)_\rho \geq n\gamma_d(h_2) - 1,$$

where $\rho_{X^n E \Theta^n} = \frac{1}{(d+1)^n} \sum_{x \in [d]^n, \Theta^n \in [d+1]^n} |x\rangle\langle x| \langle x| U_{\theta^n} \rho_{A^n E} U_{\theta^n}^\dagger |x\rangle \otimes |\theta^n\rangle\langle \theta^n|$ is the state obtained when system A^n is measured in the basis defined in the register Θ^n and

$$\gamma_d(h_2) = \begin{cases} h_2 & \text{if } h_2 \geq \frac{d-1}{d} \log(d+1) \\ f_d^{-1}(h_2) & \text{if } h_2 < \frac{d-1}{d} \log(d+1) \end{cases}$$

with $f_d(\alpha) = h(\alpha) + \alpha \log(d^2 - 1) - \log d$ defined as in Theorem 2.

Proof. We apply Theorem 1 with $\mathcal{M}_{A^n \rightarrow X^n \Theta^n} = \mathcal{N}^{\otimes n}$ where $\mathcal{N}(\rho) = \frac{1}{\sqrt{d+1}} \sum_{x \in [d], \theta \in [d+1]} |\theta\rangle\langle\theta| \otimes |x\rangle\langle x| U_\theta \rho U_\theta^\dagger |x\rangle$. Analogous to the proof of Theorem 10, it is simple to see that $2^{-H_2(X^n \Theta^n | E)_{\mathcal{M}(\rho)}} = 2^{-H_2(X^n | E \Theta^n)_\rho}$. We have in this case

$$\begin{aligned} ((\mathcal{N}^\dagger \circ \mathcal{N}) \otimes \text{id})(\Phi) &= \frac{1}{d+1} \sum_{\theta \in [d+1], x \in [d], i, j \in [d]} \langle x | U_\theta | i \rangle \langle j | U_\theta^\dagger | x \rangle U_\theta^\dagger | x \rangle \langle x | U_\theta \otimes | i \rangle \langle j | \\ &= \frac{1}{d+1} \sum_{\theta \in [d+1], x \in [d]} U_\theta^\dagger | x \rangle \langle x | U_\theta \otimes \sum_{i, j \in [d]} \langle x | U_\theta | i \rangle \langle j | U_\theta^\dagger | x \rangle | i \rangle \langle j | \\ &= \frac{1}{d+1} \sum_{\theta \in [d+1], x \in [d]} U_\theta^\dagger | x \rangle \langle x | U_\theta \otimes \top(U_\theta^\dagger | x \rangle \langle x | U_\theta), \end{aligned}$$

where Φ is the unnormalized maximally entangled state across two qudits, and \top denotes the transpose with respect to the standard basis. Now we use the fact that the states $\{U_\theta | x\rangle\}_{\theta \in [d+1], x \in [d]}$ form a state two-design [35]:

$$\sum_{\theta \in [d+1], x \in [d]} U_\theta^\dagger | x \rangle \langle x | U_\theta \otimes U_\theta^\dagger | x \rangle \langle x | U_\theta = \text{id}_{A\bar{A}} + F_{A\bar{A}},$$

where $F_{A\bar{A}}$ denotes the swap operator $F = \sum_{x, x' \in [d]} |x\rangle\langle x'| \otimes |x'\rangle\langle x|$. As $(\text{id} \otimes \top)(F) = \Phi$, we have

$$(\mathcal{N}^\dagger \circ \mathcal{N} \otimes \text{id})(\Phi) = \frac{\text{id} + \Phi}{d+1} = \frac{\Phi_0}{d+1} + \frac{\sum_{s \in [d^2]} \Phi_s}{d(d+1)} = \frac{1}{d} \left(\Phi_0 + \frac{\sum_{s \neq 0} \Phi_s}{d+1} \right).$$

This means that for the n -fold tensor product $\mathcal{M} = \mathcal{N}^{\otimes n}$, we have using the notation of Theorem 1 that $\lambda_s = \frac{1}{d^n} \frac{1}{(d+1)^{|s|}}$ for all $s \in [d^2]^n$. As a result, when applying Theorem 1, it is natural to choose the partition $\mathfrak{S}_+ \cup \mathfrak{S}_-$ of the form $\mathfrak{S}_+ = \{s \in [d^2]^n : |s| \leq \ell_0\}$ and $\mathfrak{S}_- = \{s \in [d^2]^n : |s| > \ell_0\}$ for a value of $\ell_0 \in \{0, \dots, n\}$ to be chosen as a function of h_2 . We obtain for any ℓ_0 ,

$$\begin{aligned} 2^{-H_2(X^n | E \Theta^n)_\rho} &\leq \sum_{\ell=0}^{\ell_0} \binom{n}{\ell} (d^2 - 1)^\ell 2^{-h_2 n} (d+1)^{-\ell} d^{-n} + (d+1)^{-\ell_0-1} \delta_{\ell_0 \leq n-1} \\ &= \sum_{\ell=0}^{\ell_0} \binom{n}{\ell} (d-1)^\ell 2^{-nh_2 - n \log d} + (d+1)^{-\ell_0-1} \delta_{\ell_0 \leq n-1}, \end{aligned} \quad (30)$$

where $\delta_{\ell_0 \leq n-1} = 1$ if $\ell_0 \leq n-1$ and 0 otherwise. If $h_2 \geq \frac{d-1}{d} \log(d+1)$, let $\ell_0 = n$, in which case we obtain a bound of

$$2^{-H_2(X^n | E \Theta^n)_\rho} \leq \sum_{\ell=0}^n \binom{n}{\ell} (d-1)^\ell 2^{-nh_2 - n \log d} = 2^{-h_2 n}.$$

If $h_2 < \frac{d-1}{d} \log(d+1)$, then we are going to choose $\ell_0 \leq \frac{d-1}{d} n$. Note that $f_d(\frac{d-1}{d}) = \frac{d-1}{d} \log(d+1)$. As $h_2 < \frac{d-1}{d} \log(d+1)$ and f_d is nondecreasing on $[0, (d-1)/d]$, we can find $\alpha_0 \leq (d-1)/d$ be such that $f_d(\alpha_0) = h_2$. We then choose $\ell_0 = \lfloor \alpha_0 n \rfloor$. As a result,

$$\begin{aligned} \sum_{\ell=0}^{\ell_0} \binom{n}{\ell} (d-1)^\ell 2^{-h_2 n - (\log d) n} &\leq 2^{n(h(\ell_0/n) + \ell_0/n \log(d-1)) - n(h_2 + \log d)} \\ &\leq 2^{n(h(\alpha_0) + \alpha_0 \log(d-1) - h_2 - \log d)} \\ &= 2^{n(-\alpha_0 \log(d+1) + \log d + h_2 - h_2 - \log d)} = (d+1)^{-\alpha_0 n}, \end{aligned}$$

where the first inequality is due to Lemma 25. In addition, we have $(d+1)^{-\ell_0-1} \leq (d+1)^{-\alpha_0 n}$. Using these bounds in (26), we obtain in this case

$$2^{-H_2(X^n | E \Theta^n)_\rho} \leq 2(d+1)^{-\alpha_0 n}.$$

Taking the logarithm leads to the desired result. \square

The following corollary expresses the uncertainty relation described in Theorem 12 in terms of min-entropies. The proof is the same as Corollary 11.

Corollary 13. *Using the same notation as in Theorem 12, we have*

$$H_{\min}(X^n|E\Theta^n)_\rho \geq \frac{1}{2} (n\gamma_d(h_2) - 1) \quad (31)$$

$$\geq \frac{1}{2} (n\gamma_d(h_{\min}) - 1). \quad (32)$$

where $h_{\min} = \frac{H_{\min}(A|E)_\rho}{n}$. Moreover, for any $\varepsilon \in (0, 1]$, we have

$$H_{\min}^\varepsilon(X^n|E\Theta^n)_\rho \geq n\gamma_d(h_2) - 1 - \log \frac{2}{\varepsilon^2}. \quad (33)$$

E. Security in the noisy-storage model

1. General noisy storage model

We now use our new uncertainty relations to prove that the primitive weak string erasure can be secure as soon as one of the parties has a memory that cannot reliably store n qubits. In weak string erasure, the objective is to generate a string X^n such that Alice holds X^n and Bob holds a random subset $I \subseteq [n]$ and the bits X_I of X^n corresponding to the indices in I . Randomly chosen here means that each index $i \in [n]$ has probability $1/2$ of being in I . The security criterion is that at the end of the protocol, a cheating Bob should have a state satisfying $H_{\min}(X^n|B) \geq \lambda n$ where B represents Bob's system, and a cheating Alice should not learn anything about I . To summarize all relevant parameters, we speak of an (n, λ) -WSE scheme and refer to [37] for a definition⁹. It is proved in [37] that bit commitment can be implemented using weak string erasure and classical communication.

Protocol. The protocol we use here is the same as the one of [37]. Alice prepares a random string $X^n \in \{0, 1\}^n$ and encodes each bit X_i in either the standard basis $\Theta_i = 0$ or the Hadamard basis $\Theta_i = 1$, each with probability $1/2$. Then Bob measures these qubits in randomly chosen bases Θ'_i . After the waiting time, Alice reveals both X^n and Θ^n . The set I is defined by $I = \{i : \Theta_i = \Theta'_i\}$. For a more detailed description of the protocol, we refer the reader to [37].

To state the result, we first define the notion of *channel fidelity* introduced by [5] which is perhaps the most widely used quantity to measure how good a channel is at sending quantum information. For a channel $\mathcal{N} : \mathcal{S}(Q) \rightarrow \mathcal{S}(Q')$, the channel fidelity F_c quantifies how well \mathcal{N} preserves entanglement with a reference:

$$F_c(\mathcal{N}) = F(\Phi_{Q'A}^N, [\mathcal{N} \otimes \text{id}_A](\Phi_{Q'A}^N)), \quad (34)$$

where $\Phi_{Q'A}^N$ is a normalized maximally entangled state. For example, one way of defining the (one-shot) quantum capacity with free classical forward communication of a channel $\mathcal{F}_{B \rightarrow C}$ is by the maximum of $\log |Q|$ over all encodings $\mathcal{E} : \mathcal{S}(Q) \rightarrow \mathcal{S}(B \otimes M)$ and decodings $\mathcal{D} : \mathcal{S}(C \otimes M) \rightarrow \mathcal{S}(Q')$ such that $F_c(\mathcal{D} \circ (\mathcal{F} \otimes \text{id}_M) \circ \mathcal{E}) \geq 1 - \varepsilon$ for small enough ε . Here id_M refers to a noiseless classical channel.

The following theorem states that as soon as the storage device of Bob cannot send quantum information with reliability better than η , then we can perform two-party computation securely provided $\eta \leq 2^{-\delta n}$ for any $\delta > 0$. One can even obtain security when $\eta \leq 2^{-c(\log^2 n + \log n \log(1/\varepsilon))}$ for some large enough constant c . Previously, this was only known when $\eta < 2^{-(2-\log 3)n}$ [11].

Theorem 14. *Let Bob's storage device be given by $\mathcal{F} : \mathcal{S}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{S}(B)$, and let $\eta \in (0, 1)$. Assume that we have*

$$\max_{\mathcal{D}, \mathcal{E}} F_c(\mathcal{D} \circ (\mathcal{F} \otimes \text{id}_M) \circ \mathcal{E})^2 \leq \eta \quad (35)$$

where the maximum is over all quantum channels $\mathcal{E} : \mathcal{S}((\mathbb{C}^2)^{\otimes n}) \rightarrow \mathcal{S}(\mathcal{H}_{\text{in}} \otimes M)$ and $\mathcal{D} : \mathcal{S}(B \otimes M) \rightarrow \mathcal{S}((\mathbb{C}^2)^{\otimes n})$.

Then, the protocol described above implements a (n, λ) -WSE for

$$\lambda = \frac{1}{2} \left(\gamma(-1 + \log(1/\eta)/n) - \frac{1}{n} \right).$$

⁹ Note that the original definition includes a security error ε , which in our case is $\varepsilon = 0$.

Proof. The proof of correctness of the protocol, and security against dishonest Alice is identical to [37] and does not lead to any error terms.

For the security against dishonest Bob, it is convenient to imagine a purification of the protocol, in which Alice prepares n EPR pairs $\Phi_{A^n Q}^N$, where she sends Q to Bob and later measures her n qubits A^n in randomly chosen BB84 bases. Bob's general attack is illustrated in Figure 3. We use the uncertainty relation in Equation (28), with $E = BM\Theta^n$ on $\rho_{A^n BM\Theta^n}$. In order to do that, we first derive a lower bound on $h_{\min} = \frac{H_{\min}(A^n|BM\Theta^n)_\rho}{n}$. Note that because Θ^n is independent of $A^n BM$, we have $H_{\min}(A^n|BM\Theta^n)_\rho = H_{\min}(A^n|BM)_\rho$. We now use Condition (35) to obtain a lower bound on $H_{\min}(A^n|BM)$.

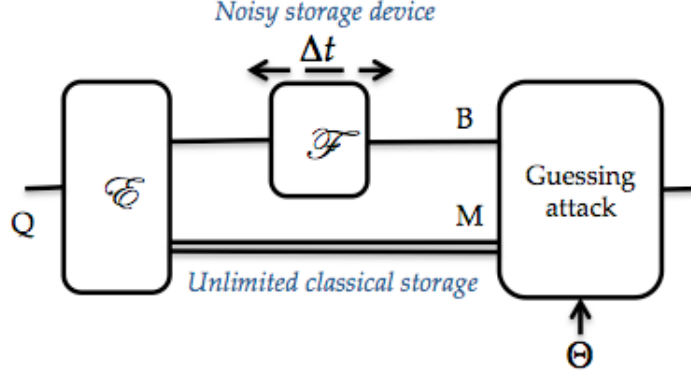


FIG. 3: An attack of dishonest Bob is described by an encoding attack \mathcal{E} and a guessing attack because for classical X^n the min-entropy $H_{\min}(X^n|BM\Theta^n)$ is directly related to the probability that Bob guesses X^n . The uncertainty relation of (32) is going to allow us to relate this guessing probability to how well a decoding attack \mathcal{D} can preserve entanglement between Alice and Bob, where \mathcal{D} acts on BM .

In fact, we use an operational interpretation of the conditional min-entropy due to [36]:

$$H_{\min}(A^n|BM)_\rho = -\log |A^n| \max_{\Lambda_{BM \rightarrow A^n}} F(\Phi_{A^n \bar{A}^n}^N, \text{id}_{A^n} \otimes \Lambda(\rho_{A^n BM}))^2, \quad (36)$$

where $\Phi_{A^n \bar{A}^n}^N$ is the normalized maximally entangled state across $A^n \bar{A}^n$. That is, the min-entropy is directly related to the “amount” of entanglement between A^n and BM . The map Λ in (36) can be understood as a decoding attack \mathcal{D} aiming to restore entanglement with Alice.

Further, note that the expression in (36) is the same as

$$\max_{\mathcal{D}, \mathcal{E}} F(\Phi_{A^n B}^N, \text{id}_{A^n} \otimes [\mathcal{D} \circ (\mathcal{F} \otimes \text{id}_M) \circ \mathcal{E}](\Phi_{A^n Q}^N)) = \max_{\mathcal{D}, \mathcal{E}} F_c(\mathcal{D} \circ (\mathcal{F} \otimes \text{id}_M) \circ \mathcal{E}). \quad (37)$$

By the assumption on the storage device \mathcal{F} , we obtain that for any encoding \mathcal{E} and decoding \mathcal{D} attack of Bob

$$\begin{aligned} H_{\min}(A^n|BM)_\rho &\geq -\log 2^n F_c(\mathcal{D} \circ (\mathcal{F} \otimes \text{id}_M) \circ \mathcal{E})^2 \\ &\geq -(n - \log(1/\eta)). \end{aligned}$$

Then, using the uncertainty relation of (28), we obtain

$$H_{\min}(X^n|BM\Theta^n)_\rho \geq \frac{1}{2} (n\gamma (-1 + \log(1/\eta)/n) - 1),$$

which proves the desired result. \square

2. Special case: bounded storage model

The next theorem simply states the result in the important special case of the bounded storage model.

Theorem 15 (WSE in the bounded storage model). *If Alice has q qubits of quantum memory then the protocol described in the previous section implements (n, λ) -WSE with $\lambda = \frac{1}{2} (\gamma(-q/n) - \frac{1}{n})$.*

Proof. The proof is the same as Theorem 14, but we can now directly obtain a lower bound on $H_2(A^n|BM)_\rho \geq -q$ using Lemma 23. By (27), we have

$$H_{\min}(X^n|BM\Theta^n)_\rho \geq \frac{1}{2}(n\gamma(-q/n) - 1).$$

□

Previously, in this case, security was only proven when $q < \frac{2n}{3}$ [42] with a variant of this protocol that uses a six-state encoding. Using the estimate in Claim 24, the previous theorem shows that $q < n - c \log^2 n$ for some large enough c would be sufficient to perform WSE securely. Using the construction of [37], this leads to a secure bit commitment provided $q < n - c \log^2 n - c \log n \log(1/\varepsilon)$ for some large enough constant c and where ε is the failure probability.

V. CONCLUSION

We have determined a bound on how the min-entropy changes when A is transformed to $\mathcal{M}(A)$ for a certain general class of processes \mathcal{M} . Our results on entanglement sampling, as well as uncertainty relations with respect to quantum side information then follow naturally for different choices of \mathcal{M} . Our results on entanglement sampling have in fact already found applications in the context of studying properties of random quantum circuits [13].

One important aspect of our results compared to previous works on uncertainty relations and quantum random access codes is to give nontrivial bounds for all the range of possible min-entropy of the input. However, for some specific ranges of the input entropy, other techniques lead to better rates. It would be interesting to see if it is possible to combine our techniques with ideas from previous work such as [11] for uncertainty relations or [6] for random access codes to obtain tight bounds. It is likely that other interesting statements can be made using Theorem 1 for different maps, and it is an interesting open question to extend our results to more general maps.

Acknowledgments

We thank Oleg Szehr, Marco Tomamichel and Thomas Vidick for useful discussions. OF is supported by the European Research Council grant No. 258932. SW thanks ETH Zürich for their hospitality. SW is supported by the National Research Foundation and the Ministry of Education, Singapore. FD acknowledges support from the Danish National Research Foundation and The National Science Foundation of China (under the grant 61061130540) for the Sino-Danish Center for the Theory of Interactive Computation, within which part of this work was performed; and also from the CFEM research center (supported by the Danish Strategic Research Council) within which part of this work was performed.

-
- [1] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter. The mother of all protocols: Restructuring quantum information's family tree. *Proceedings of Royal Society A*, 465:2537, 2009. [arXiv:quant-ph/0606225](#).
 - [2] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *J. ACM*, 49(4):496–511, 2002. [arXiv:quant-ph/9804043](#).
 - [3] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002. [arXiv:quant-ph/0103162](#).
 - [4] H. Barnum and E. Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *J. Math. Phys.*, 43:2097, 2002.
 - [5] H. Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. *IEEE Trans. Inform. Theory*, 46:1317–1329, 2000. [arXiv:quant-ph/9809010](#).
 - [6] A. Ben-Aroya, O. Regev, and R. de Wolf. A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In *Proc. IEEE FOCS*, 2008. [arXiv:0705.3806](#).
 - [7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. International Conference on Computers, Systems and Signal Processing*, 1984.
 - [8] M. Berta, F. Brandao, M. Christandl, and S. Wehner. Entanglement cost of quantum channels. [arXiv:1108.5357](#), 2011.
 - [9] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nat. Phys.*, 6:659, 2010. [arXiv:0909.0950](#).
 - [10] M. Berta, P. Coles, and S. Wehner. An equality between entanglement and uncertainty. 2013. [arXiv:1302.5902](#).

- [11] M. Berta, O. Fawzi, and S. Wehner. Quantum to classical randomness extractors. In *Proc. CRYPTO*, volume 7417 of *LNCS*, pages 776–793. Springer Verlag, 2012. [arXiv:1111.2026](#).
- [12] Niek J. Bouman, Serge Fehr, Carlos González-Guillén, and Christian Schaffner. An all-but-one entropic uncertainty relation, and application to password-based identification. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 7582 of *Lecture Notes in Computer Science*, pages 29–44. Springer Berlin Heidelberg, 2013. [arXiv:1105.6212](#).
- [13] W. Brown and O. Fawzi. Decoupling with small-depth random quantum circuits. 2013. in preparation.
- [14] H. Buhrman, M. Christandl, P. Hayden, H. K. Lo, and S. Wehner. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Phys. Rev. A*, 78(2):22316, 2008. [arXiv:quant-ph/0504078](#).
- [15] H. Buhrman, M. Christandl, and C. Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Phys. Rev. Lett.*, 109:160501, 2012. [arXiv:1201.0849](#).
- [16] C. Cachin and U. M. Maurer. Unconditional security against memory-bounded adversaries. In *Proc. CRYPTO*, volume 1294 of *LNCS*, pages 292–306, 1997.
- [17] H.F. Chau and H-K. Lo. Making an empty promise with a quantum computer. *Fortschritte der Physik*, 46:507–520, 1998. Republished in ‘Quantum Computing, where do we want to go tomorrow?’ edited by S. Braunstein, [arXiv:quant-ph/9709053](#).
- [18] I. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Proc. CRYPTO*, volume 4622 of *LNCS*, pages 360–378, 2007. [arXiv:quant-ph/0612014](#).
- [19] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *Proc. IEEE FOCS*, pages 449–458, 2005. [arXiv:quant-ph/0508222](#).
- [20] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and QKD in the bounded-quantum-storage model. In *Proc. CRYPTO*, Springer Lecture Notes in Computer Science, pages 342–359, 2007. [arXiv:0708.2557](#).
- [21] G. D’Ariano, D. Kretschmann, D. Schlingemann, and R.F. Werner. Quantum bit commitment revisited: the possible and the impossible. *Phys. Rev. A*, 76:032328, 2007. [arXiv:quant-ph/0605224](#).
- [22] L. del Rio, J. Aberg, R. Renner, O. Dahlsten, and V. Vedral. The thermodynamic meaning of negative entropy. *Nature*, 474:61–64, 2011.
- [23] L. del Rio, A. Hutter, R. Renner, and S. Wehner. Relative thermalization. In preparation, 2013.
- [24] F. Dupuis. *The decoupling approach to quantum information theory*. PhD thesis, Université de Montreal, 2010. [arXiv:1004.1641](#).
- [25] F. Dupuis, M. Berta, J. Wullschlegler, and R. Renner. One-shot decoupling. 2010. [arXiv:1012.6044](#).
- [26] S. Dziembowski and U. Maurer. On generating the initial key in the bounded-storage model. In *Proc. EUROCRYPT*, volume 3027 of *LNCS*, pages 126–137, 2004.
- [27] V. Guruswami. [Introduction to Coding Theory, course notes](#). 2010.
- [28] P. Hausladen and W. Wootters. A pretty good measurement for distinguishing quantum states. *J. Mod. Optic.*, 41(12):2385–2390, 1994.
- [29] M. Hayashi. *Quantum information*. Springer, 2006.
- [30] P. Hayden, M. Horodecki, J. Yard, and A. Winter. A decoupling approach to the quantum capacity. *Open Systems and Information Dynamics*, 15:7–19, 2008. [arXiv:quant-ph/0702005](#).
- [31] P. Hayden and J. Preskill. Black holes as mirrors: quantum information in random subsystems. *J. High Energy Phys.*, page 120, 2007. [arXiv:0708.4025](#).
- [32] M. Horodecki, J. Oppenheim, and A. Winter. Quantum state merging and negative information. *Comm. Math. Phys.*, 269:107, 2006. [arXiv:quant-ph/0512247v1](#).
- [33] A. Hutter. [Understanding Equipartition and Thermalization from Decoupling](#), 2011.
- [34] R. Impagliazzo, L. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proc. ACM STOC*, pages 12–24. ACM, 1989.
- [35] A. Klappenecker and M. Rotteler. Mutually unbiased bases are complex projective 2-designs. In *Proc. IEEE ISIT*, pages 1740–1744, 2005. [arXiv:quant-ph/0502031](#).
- [36] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inform. Theory*, 55:4674–4681, 2009. [arXiv:0807.1338](#).
- [37] R. König, S. Wehner, and J. Wullschlegler. Unconditional security from noisy quantum storage. *IEEE Trans. Inform. Theory*, 58(3):1962–1984, 2012. [arXiv:0906.1030](#).
- [38] R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. *IEEE Trans. Inform. Theory*, 57(7):4760–4787, 2011. [arXiv:0712.4291](#).
- [39] N. Linden, S. Popescu, A.J. Short, and A. Winter. Quantum mechanical evolution towards thermal equilibrium. *Phys. Rev. E.*, page 061103, 2009.
- [40] H-K. Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154, 1997.
- [41] H-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410, 1997.
- [42] P. Mandayam and S. Wehner. Achieving the physical limits of the bounded-storage model. *Phys. Rev. A*, 83:022329, 2011. [arXiv:1009.1596](#).
- [43] U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *J. Cryptol.*, 5:53–66, 1992.
- [44] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, 1997.
- [45] A. Nayak. Dense quantum coding and a lower bound for 1-way quantum automata. In *Proc. ACM STOC*, pages 369–377, 1999.
- [46] N. Ng, S. Joshi, C. Chia, C. Kurtsiefer, and S. Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Comm.*, 3:1326, 2012.
- [47] N. Nisan and D. Zuckerman. Randomness is linear in space. *J. Comput. Syst. Sci.*, 52(1):43 – 52, 1996.

- [48] S. Popescu, A. J. Short, and A. Winter. Entanglement and the foundations of statistical mechanics. *Nat. Phys.*, 2:754–758, 2006.
- [49] R. Prevedel, D. Hamel, R. Colbeck, K. Fisher, and K. Resch. Experimental investigation of the uncertainty principle in the presence of quantum memory and its application to witnessing entanglement. *Nat. Phys.*, 7:757–761, 2011.
- [50] R. Renner. Security of quantum key distribution. *Int. J. Quantum Inf.*, 6:1, 2008. [arXiv:quant-ph/0512258](#).
- [51] C. Schaffner, B. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Inf. Comput.*, 9:11, 2008. [arXiv:0807.1333](#).
- [52] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner. Decoupling with unitary almost two-designs. 2011. [arXiv:1109.4348](#).
- [53] K. Temme and M. Kastoryano. Quantum logarithmic sobolev inequalities and rapid mixing. 2012. [arXiv:1207.3261](#).
- [54] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zürich, 2012. [arXiv:1203.2142](#).
- [55] M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. *IEEE Trans. Inform. Theory*, 55:5840–5847, 2009. [arXiv:0811.1221](#).
- [56] M. Tomamichel, C.C.W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nat. Comm.*, 3:634, 2012.
- [57] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106(11):110506, 2011. [arXiv:1009.2015](#).
- [58] S. Vadhan. [Pseudorandomness](#).
- [59] S. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *J. Cryptol.*, 17:43–77, 2004.
- [60] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, 2008. [arXiv:0711.2895](#).
- [61] S. Wehner and A. Winter. Entropic uncertainty relations—a survey. *New J. Phys.*, 12:025009, 2010. [arXiv:0907.3704](#).
- [62] Michael Wolf. [Quantum channels and operations, guided tour](#). 2012.
- [63] J. Wullschlegel. Bitwise quantum min-entropy sampling and new lower bounds for random access codes. 2010. [arXiv:1012.2291](#).
- [64] A. C.-C. Yao. Security of quantum protocols against coherent measurements. In *Proc. ACM STOC*, pages 67–75, 1995.

Appendix A: Technical Lemmas

Lemma 3. For any $\ell_0 \in \{0, \dots, n\}$ such that $\ell_0 \leq \frac{d^2-1}{d^2}n$ where $d^2 < n$, we have

$$\sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell \leq n^2 \binom{n}{\ell_0} (d^2-1)^{\ell_0} \max\left(\frac{n-\ell_0-1}{n}, \frac{1}{d^2}\right)^k.$$

Proof. It is convenient to study separately the case where $\ell_0 \leq \frac{d^2-1}{d^2}(n-k)$ and the case where $\ell_0 > \frac{d^2-1}{d^2}(n-k)$. More precisely, the following claim introduces the value k_0 that separates these two cases.

Claim 16. There exists $k_0 \in \{1, \dots, n\}$ such that $\ell_0 \leq \frac{d^2-1}{d^2}(n-k_0+1)$ such that

1. for $k \leq k_0$, $\sum_{\ell \leq \ell_0} \binom{n-k}{\ell} (d^2-1)^\ell \leq n \cdot \binom{n-k}{\ell_0} (d^2-1)^{\ell_0}$,
2. and $\sum_{\ell \leq n-k_0} \binom{n-k_0}{\ell} (d^2-1)^\ell = (d^2)^{n-k_0} \leq n \cdot \binom{n-k_0}{\ell_0} (d^2-1)^{\ell_0}$.

Proof. We have for $\ell \geq 1$,

$$\frac{\binom{n-k}{\ell} (d^2-1)^\ell}{\binom{n-k}{\ell-1} (d^2-1)^{\ell-1}} = (d^2-1) \frac{n-k-\ell+1}{\ell}.$$

Now define $\ell_{\max}(k)$ to be the largest integer such that $\ell_{\max}(k) \leq \frac{d^2-1}{d^2}(n-k+1)$. In this case, we have for $\ell \leq \ell_{\max}(k)$, $(d^2-1) \frac{n-k-\ell+1}{\ell} \geq 1$. As a result, we have that for a fixed k , the expression $\binom{n-k}{\ell} (d^2-1)^\ell$ is increasing for $\ell \leq \ell_{\max}(k)$. In addition, if $\ell > \ell_{\max}(k)$, then $\ell > \frac{d^2-1}{d^2}(n-k+1)$ which means that for $\ell > \ell_{\max}(k)$, the expression $\binom{n-k}{\ell} (d^2-1)^\ell$ is decreasing.

We choose k_0 to be the largest integer such that $\ell_0 \leq \frac{d^2-1}{d^2}(n-k_0+1)$. Note that such a k_0 exists because we assumed $\ell_0 \leq \frac{d^2-1}{d^2}n$. This means that $\ell_0 > \frac{d^2-1}{d^2}(n-k_0) \geq \frac{d^2-1}{d^2}(n-k_0+1) - 1$. This implies that $\ell_0 = \ell_{\max}(k_0)$ is the maximum of $\binom{n-k_0}{\ell} (d^2-1)^\ell$ over $\ell \in \{0, \dots, n-k_0\}$. Both points then follows from bounding the sum by n times the largest term. \square

As a result, we have for $k \leq k_0$,

$$\begin{aligned} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell &\leq n \cdot \binom{n-k}{\ell_0} (d^2-1)^{\ell_0} \\ &= n \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} \frac{(n-\ell_0) \cdots (n-\ell_0-k+1)}{n \cdots (n-k+1)}. \end{aligned}$$

Note that for $k = 1$, the result simply follows from the fact that $n-\ell_0-1 \geq 1$, which itself comes from our assumptions $\ell_0 \leq \frac{d^2-1}{d^2}n$ and $d^2 < n$. For $k > 1$, we can continue with

$$\begin{aligned} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell &\leq n \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} (n-\ell_0) \frac{(n-\ell_0-1) \cdots (n-\ell_0-k+1)}{n \cdots (n-k+1)} \\ &\leq n^2 \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} \left(\frac{n-\ell_0-1}{n} \right)^k. \end{aligned}$$

For $k > k_0$,

$$\begin{aligned} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell &\leq d^{2(n-k)} \\ &\leq n \cdot \binom{n-k_0}{\ell_0} (d^2-1)^{\ell_0} d^{-2(k-k_0)} \\ &= n \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} \frac{(n-\ell_0) \cdots (n-\ell_0-k_0+1)}{n \cdots (n-k_0+1)} \left(\frac{1}{d^2} \right)^{k-k_0}. \end{aligned} \tag{A1}$$

For $k_0 > 1$, we use the fact that $\ell_0 \leq \frac{d^2-1}{d^2}(n-k_0+1)$, which implies that $\frac{1}{d^2} \leq \frac{n-\ell_0-k_0+1}{n-k_0+1}$. Thus,

$$\begin{aligned} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell &\leq d^{2(n-k)} \\ &\leq n \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} \frac{(n-\ell_0) \cdots (n-\ell_0-k_0+1)^{(k-k_0)+1}}{n \cdots (n-k_0+1)^{(k-k_0)+1}} \\ &\leq n \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} (n-\ell_0) \left(\frac{n-\ell_0-1}{n} \right)^k \\ &\leq n^2 \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} \left(\frac{n-\ell_0-1}{n} \right)^k. \end{aligned}$$

For $k_0 = 1$, (A1) becomes

$$\begin{aligned} \sum_{\ell=0}^{\ell_0} \binom{n-k}{\ell} (d^2-1)^\ell &\leq n \cdot \binom{n}{\ell_0} (d^2-1)^{\ell_0} \frac{n-\ell_0}{n} \left(\frac{1}{d^2} \right)^{k-1} \\ &\leq n^2 \binom{n}{\ell_0} (d^2-1)^{\ell_0} \left(\frac{1}{d^2} \right)^k, \end{aligned}$$

using the assumption $n > d^2$. □

Appendix B: Some useful properties of entropy measures

Lemma 17. Let $\rho_{AB} \in \mathcal{S}_{\leq}(AB)$. Then, $H_{\min}(A|B)_\rho \leq H_2(A|B)_\rho \leq 2H_{\min}(A|B)_\rho + \log d_A$.

Proof. The first inequality can be proven as follows:

$$\begin{aligned} 2^{-H_{\min}(A|B)_\rho} &= \max_{E_{AB}: E_B = \text{id}_B} \text{Tr}[E_{AB} \rho_{AB}] \\ &\geq \text{Tr}[(\rho_B^{-1/2} \rho_{AB} \rho_B^{-1/2}) \rho_{AB}] \\ &= 2^{-H_2(A|B)_\rho}. \end{aligned}$$

For the second inequality, we proceed as follows. By [36], there exists a CPTP map $\mathcal{E}_{B \rightarrow A'}$ with $A' \cong A$, such that $H_{\min}(A|B)_\rho = H_{\min}(A|A')_{\mathcal{E}(\rho)}$. Letting $\tilde{\rho} = \mathcal{E}(\rho)$ and $\omega_{A'} = \sqrt{\tilde{\rho}_{A'}} / \text{Tr}[\sqrt{\tilde{\rho}_{A'}}]$, we get

$$\begin{aligned} 2^{-H_{\min}(A|B)_\rho} &= 2^{-H_{\min}(A|A')_{\tilde{\rho}}} \\ &\leq 2^{-H_{\min}(A|A')_{\tilde{\rho}|\omega}} \\ &= \left\| \omega_{A'}^{-1/2} \tilde{\rho}_{AA'} \omega_{A'}^{-1/2} \right\|_\infty \\ &= \left\| \tilde{\rho}_{A'}^{-1/4} \tilde{\rho}_{AA'} \tilde{\rho}_{A'}^{-1/4} \right\|_\infty \text{Tr}[\sqrt{\tilde{\rho}_{A'}}] \\ &\leq \left\| \tilde{\rho}_{A'}^{-1/4} \tilde{\rho}_{AA'} \tilde{\rho}_{A'}^{-1/4} \right\|_2 \text{Tr}[\sqrt{\tilde{\rho}_{A'}}] \\ &= \sqrt{2^{-H_2(A|A')_{\tilde{\rho}|\tilde{\rho}}}} \text{Tr}[\sqrt{\tilde{\rho}_{A'}}] \\ &\leq \sqrt{2^{-H_2(A|B)_\rho}} \text{Tr}[\sqrt{\tilde{\rho}_{A'}}] \\ &\leq \sqrt{d_A 2^{-H_2(A|B)_\rho}}, \end{aligned}$$

and the lemma follows. \square

Lemma 18. Let $\rho_{XB} \in \mathcal{S}_{\leq}(XB)$ be a CQ state, and let $\sigma \in \mathcal{S}_{\leq}(B)$ be such that $H_{\min}(X|B)_\rho = H_{\min}(X|B)_{\rho|\sigma}$. Then

$$H_{\min}(X|B)_\rho \leq H_2(X|B)_\rho \leq 2H_{\min}(X|B)_\rho.$$

Proof. The lower bound is a special case of Lemma 17. For the upper bound, from the operational interpretation of H_{\min} , we get that there exists a measurement $\mathcal{M}_{B \rightarrow X'}$ such that $H_{\min}(X|B)_\rho = H_{\min}(X|X')_{\mathcal{M}(\rho)}$. Using this, we get that

$$\begin{aligned} 2^{-H_{\min}(X|B)_\rho} &= 2^{-H_{\min}(X|X')_{\mathcal{M}(\rho)}} \\ &= \mathbb{E}_{\tilde{X}'} 2^{-H_{\min}(X|X'=\tilde{X}')_{\mathcal{M}(\rho)}} \\ &\leq \mathbb{E}_{\tilde{X}'} 2^{-\frac{1}{2}H_2(X|X'=\tilde{X}')_{\mathcal{M}(\rho)}} \\ &\leq \sqrt{\mathbb{E}_{\tilde{X}'} 2^{-H_2(X|X'=\tilde{X}')_{\mathcal{M}(\rho)}}} \\ &= \sqrt{2^{-H_2(X|X')_{\mathcal{M}(\rho)|\mathcal{M}(\rho)}}} \\ &\leq \sqrt{2^{-H_2(X|B)_\rho}}, \end{aligned}$$

where the first inequality follows from an application of Cauchy-Schwarz, the second from the concavity of the square root, and the third from the monotonicity of H_2 under CPTP maps. The last equality is due to the following:

$$\begin{aligned} \mathbb{E}_{\tilde{X}'} 2^{-H_2(X|X'=\tilde{X}')_{\mathcal{M}(\rho)}} &= \sum_{x'} \mathbf{Pr}\{X' = x'\} \sum_x \mathbf{Pr}\{X = x|X' = x'\}^2 \\ &= \text{Tr}\left[\left((\text{id}_X \otimes \rho_{X'}^{-1/4}) \rho_{XX'} (\text{id}_X \otimes \rho_{X'}^{-1/4})\right)^2\right] \\ &= 2^{-H_2(X|X')_{\mathcal{M}(\rho)|\mathcal{M}(\rho)}}. \end{aligned}$$

\square

Lemma 19. Let $\rho_{AB} \in \mathcal{S}_{\leq}(AB)$. Then, $H_2(A|B)_\rho \leq H_{\min}^\varepsilon(A|B)_\rho + \log \frac{2}{\varepsilon^2}$.

This lemma is very similar to Theorem 7 in [55], but note that they use a slightly different definition of H_2 . The proof of this version of the lemma is, therefore, very similar to theirs.

Proof. First, note that $H_{\min}^\varepsilon(A|B)_\rho \geq H_{\min}^\varepsilon(A|B)_{\rho|_\rho}$. Let $\Delta = (\rho_{AB} - 2^{-H_{\min}^\varepsilon(A|B)_{\rho|_\rho}} \text{id}_A \otimes \rho_B)_+$ (where $(\cdot)_+$ denotes the nonnegative part of an operator). Let $\lambda > 0$ be such that $H_{\min}^\varepsilon(A|B)_{\rho|_\rho} \geq -\log \lambda$ and $\varepsilon = \sqrt{2 \text{Tr}[\Delta]}$ (such a λ exists by Lemma 15 of [55]). Furthermore, let P be the projector onto the support of Δ . We then have that

$$\begin{aligned} P\rho_{AB}P &\geq \lambda P(\text{id}_A \otimes \rho_B)P \\ (P\rho_B P)^{-1/2} P\rho_{AB}P (P\rho_B P)^{-1/2} &\geq \lambda P_{AB}, \end{aligned}$$

where we have omitted the id_A 's in the second line. Using this, we get that

$$\begin{aligned} \frac{\varepsilon^2}{2} &= \text{Tr}[\Delta] \\ &= \text{Tr}[P(\rho_{AB} - \lambda \text{id}_A \otimes \rho_B)P] \\ &\leq \text{Tr}[P\rho_{AB}P] \\ &\leq \lambda^{-1} \text{Tr}[P\rho_{AB}P(P\rho_B P)^{-1/2} P\rho_{AB}P(P\rho_B P)^{-1/2}] \\ &= \lambda^{-1} 2^{D_2(P\rho_{AB}P \| P(\text{id}_A \otimes \rho_B)P)} \\ &\leq \lambda^{-1} 2^{D_2(\rho_{AB} \| \text{id}_A \otimes \rho_B)} \\ &\leq 2^{H_{\min}^\varepsilon(A|B)_\rho - H_2(A|B)_\rho}, \end{aligned}$$

where D_2 is defined in Definition 20 and the last inequality is due to Theorem 21. \square

Definition 20. Let $D_2(X\|Y)$ be defined as

$$2^{D_2(X\|Y)} := \text{Tr}[(Y^{-1/4}XY^{-1/4})^2].$$

Theorem 21. $D_2(\mathcal{E}(X)\|\mathcal{E}(Y)) \leq D_2(X\|Y)$ for any CPTP map \mathcal{E} .

Proof. Consider the map $(L, R) \mapsto LR^{-1/2}L \otimes R^{-1/2}$. Theorem 5.14 in [62] shows that it is jointly operator convex, by taking $g(R) = R^{1/2} \otimes (R^{1/2})^\top$ (which is operator concave by [62, Corollary 5.5, point 1]), $h(L) = L \otimes \text{id}$, $f(x) = x^2$. This entails that $(L, R) \mapsto \text{Tr}[R^{-1/2}LR^{-1/2}L]$ is also jointly operator convex, via the fact that

$$\text{Tr}[R^{-1/2}LR^{-1/2}L] = \text{Tr}[\Phi(LR^{-1/2}L \otimes (R^{-1/2})^\top)].$$

We now invoke Theorem 5.16 from [62] on this functional to conclude the proof. \square

Defining $H_2(A|B)_{\rho|\sigma}$ naturally as $H_2(A|B)_{\rho|\sigma} = \text{Tr} \left[\left(\sigma_B^{-1/4} \rho_{AB} \sigma_B^{-1/4} \right)^2 \right]$, we obtain the following corollary.

Corollary 22. Let $\rho_{AB} \in \mathcal{S}_{\leq}(AB)$ and $\sigma_B \in \mathcal{S}_{\leq}(B)$ such that ρ_B is in the support of σ_B . Then, for any CPTP map $\mathcal{E}_{B \rightarrow C}$, we have that $H_2(A|B)_{\rho|\sigma} \leq H_2(A|C)_{\mathcal{E}(\rho)|\mathcal{E}(\sigma)}$.

Lemma 23. Suppose $\rho \in \mathcal{S}(AQC)$ is such that the C system is classical, i.e., $\rho_{AQC} = \sum_c p(c) |c\rangle\langle c| \otimes \rho_{AQ}^c$ for some probability distribution p and orthogonal vectors $\{|c\rangle\}_c$ in C . Then

$$H_2(A|QC)_\rho = -\log \sum_c p(c) 2^{-H_2(A|Q)_{\rho^c}}.$$

In particular $H_2(A|QC) \geq -\log |Q|$.

Proof. We have

$$\begin{aligned} &\text{Tr} \left[\left(\text{id}_A \otimes \rho_{QC}^{-1/4} \rho_{AQC} \text{id}_A \otimes \rho_{QC}^{-1/4} \right)^2 \right] \\ &= \text{Tr} \left[\left(\text{id}_A \otimes \left(\sum_c p(c) |c\rangle\langle c| \otimes \rho_Q^c \right)^{-1/4} \left(\sum_c p(c) |c\rangle\langle c| \otimes \rho_{AQ}^c \right) \text{id}_A \otimes \left(\sum_c p(c) |c\rangle\langle c| \otimes \rho_Q^c \right)^{-1/4} \right)^2 \right] \\ &= \sum_c \text{Tr} \left[\left(\text{id}_A \otimes (p(c) \rho_Q^c)^{-1/4} \rho_{AQ}^c \text{id}_A \otimes (p(c) \rho_Q^c)^{-1/4} \right)^2 \right] \\ &= \sum_c p(c) \text{Tr} \left[\left(\text{id}_A \otimes (\rho_Q^c)^{-1/4} \rho_{AQ}^c \text{id}_A \otimes (\rho_Q^c)^{-1/4} \right)^2 \right]. \end{aligned}$$

To conclude the proof, we simply observe that $\text{Tr} \left[(\text{id}_A \otimes (\rho_Q)^{-1/4} \rho_{AQ} \text{id}_A \otimes (\rho_Q)^{-1/4})^2 \right] \leq \text{Tr}[\text{id}_A \otimes \rho_Q^{-1} \rho_{AQ}] = \text{Tr}[\rho_Q^{-1} \rho_Q] = |Q|$. \square

The following claim gives a bound on the function γ from Theorem 10 for small values of h_2 .

Claim 24. Write $h_2 = -1 + x$ with $x \leq 1/3$, then we have

$$\gamma(-1 + x) \geq \frac{x}{10 \log(1/x)}.$$

Proof. Recall that γ is the inverse of $g(x) = h(x) + x - 1$. We have

$$\begin{aligned} g\left(\frac{x}{10 \log(1/x)}\right) &= h\left(\frac{x}{10 \log(1/x)}\right) + \frac{x}{10 \log(1/x)} - 1 \\ &\leq 2 \cdot \frac{x}{10 \log(1/x)} \log \frac{10 \log(1/x)}{x} + \frac{x}{10 \log(1/x)} - 1 \\ &\leq \frac{x}{5 \log(1/x)} \left(\log 10 + \log \log(1/x) + \log(1/x) + \frac{1}{2} \right) - 1 \\ &\leq x - 1, \end{aligned}$$

which proves the desired result. \square

Lemma 25. Let a be a positive integer. We have for any $\ell \leq \frac{a}{a+1}$,

$$\sum_{k=0}^{\ell} \binom{n}{k} a^k \leq 2^{nh(\ell/n)} a^{\ell}$$

Proof. See for example [27], Lemma 5. \square

Appendix C: Operational interpretation of H_2

When X is classical, then it is already known [14] that

$$H_2(X|E) = -\log P_{\text{guess}}^{\text{pg}}(X|E),$$

where $P_{\text{guess}}^{\text{pg}}$ is the guessing probability using the pretty good measurement which performs very well [28]. For completeness, we here include the arguments of [10] regarding the operational interpretation of H_2 for quantum information A . Like the min-entropy, it is a natural measure of the entanglement between A and B in that $H_2(A|B) = -\log[|A| F^{\text{pg}}(A|B)^2]$ with

$$F^{\text{pg}}(A|B) = F(\Phi_{AA'}, \text{id}_A \otimes \Lambda_{B \rightarrow A'}^{\text{pg}}(\rho_{AB})), \quad (\text{C1})$$

and $\Lambda_{B \rightarrow A'}^{\text{pg}}$ is the pretty good recovery map [4]. To see this, we note that the pretty good recovery map can be written as

$$\Lambda_{B \rightarrow A'}^{\text{pg}}(\cdot) = \frac{1}{|A|} \cdot \mathcal{E}_{B \rightarrow A'}^{\dagger} \left(\rho_B^{-1/2}(\cdot) \rho_B^{-1/2} \right),$$

where $\mathcal{E}_{B \rightarrow A'}^{\dagger}$ denotes the adjoint of the Choi-Jamiołkowski map of ρ_{AB} ,

$$\mathcal{E}_{A \rightarrow B}(\cdot) = |A| \cdot \text{Tr}_A \left[((\cdot)^T \otimes \text{id}_B) \rho_{AB} \right].$$

Putting this in (4) we arrive at (C1). The map $\Lambda_{B \rightarrow A'}^{\text{pg}}$ is pretty good in the sense that it is close to optimal for recovering the maximally entangled state, i.e., the following bound holds [4]

$$F^2(A|B) \leq F^{\text{pg}}(A|B) \leq F(A|B),$$

where $F(A|B)$ is the fidelity achievable by the optimal map given in (1).